# IT risk assessment: summary report

## Sheffield City Council

**Audit 2011/12**

**The Audit Commission is an independent watchdog, driving economy, efficiency and effectiveness in local public services to deliver better outcomes for everyone.**

**Our work across local government, health, housing, community safety and fire and rescue services means that we have a unique perspective. We promote value for money for taxpayers, auditing the £200 billion spent by 11,000 local public bodies.**

**As a force for improvement, we work in partnership to assess local public services and make practical recommendations for promoting a better quality of life for local people.**

# Contents

# Introduction, scope and approach

1 As part of our work to support the opinion which we give on your accounts, we undertake an annual Information Technology (IT) risk assessment of your IT arrangements. This with other work enables us to comply with the requirements of International Standard of Audit (ISA) 315.

2 The scope of our review was to complete an IT Risk Assessment (ITRA) which included testing some general IT controls for the operation of the main financial systems and associated infrastructure.

3 The risk assessment was completed through interviews with staff from both Sheffield City Council and Capita Business Services and an examination of relevant documentation when provided. The assessment covered five main sections as below.

- IT Entity Level Controls.
- Access Security Control.
- Data Centre and Network Controls.
- Program Change Controls, New Systems Acquisition and Development.
- End User Computing (EUC).

4 Our overall conclusion in both 2010/11 and 2011/12 is that there are no significant risks identified in our review of the above sections which may impact or result in a material misstatement to the accounts. However our work during 2010/11 identified six key areas with scope for improvement and we issued and agreed a report and action plan with officers in January 2011.

5 Our follow up work in 2011/12 has identified progress has been made in introducing arrangements to address these recommendations. We have updated the action plan in Appendix 1 to reflect the position as identified during the work.

6 To place the recommendations into context we have included the 2010/11 summary report in appendix 2.

7 A small number of recommendations require residual work; the Authority needs to revisit the report and introduce arrangements that address the recommendations raised in our 2010/11 report that have not yet been fully implemented.

# Appendix 1 Action plan

The table below contains the agreed recommendations from our 2010/11 report, updated for the findings identified in our audit review during 2011/12 (and also changes to notified to us of responsible officers).

| Recommendations | |
|---|---|
| **Recommendation 1** | |
| An IS/IT strategy should be developed which clearly documents the way forward including the expected cash releasing savings and how the outsourced contract will be monitored and regularly reported to the Council. | |
| **Responsibility** | Steve Roberts (BIS SMT/Paul Green) |
| **Priority** | Medium |
| **Date** | Delivery for 31 March 2011 |
| **2010/11 Authority Comments** | A strategy will be developed that covers our vision; objectives; outcomes; performance measures; and linkages to Corporate and Business plans. |
| **2011/12 Audit update** | An IS/IT strategy has not yet been completed. BIS inform us that no date has been fixed due to ongoing discussions about a possible contract extension with Capita, and possible merging of BIS with the Council's Transformation team. |
| **Recommendation 2** | |
| The procedure for disabling the user accounts of users of Council ICT leaving the employment of the Council should be re-designed to ensure it is more timely and complete. This should include a checklist to ensure all IT equipment is collected, for example, any two factor remote access devices, mobile devices and laptops. | |
| **Responsibility** | Capita (David Cunningham) / BIS (Norma Shaw)/BIS P&P Assurance |
| **Priority** | Medium |
| **Date** | Delivery for 31 March 2011 |
| **2010/11 Authority Comments** | The existing process will be reviewed and redesigned by Capita & BIS (with BIS assurance). The process design will include engagement with HR system / information owners - to ensure business process is aligned with redesigned ICT process. |
| **2011/12 Audit update** | Some action has been taken but there still remains scope for improvement in this area. Capita users of Council ICT have expressed some concerns that the end of month HR/payroll leavers report used as a compensating control to identify leaver accounts is not accurate. |

| Recommendations | |
|---|---|
| | There is also evidence to show that user accounts belonging to users of Council ICT who have left the employment of the Council have been used since their departure.<br>Officers have commented that a review is already underway by BIS P&P Assurance on the processes within SCC and Capita. This review has identified a further significant area of concern, namely users who are not employed by SCC (contractors, consultants, NHS or agency staff etc) who are granted legitimate access but whose records (especially leaving dates) are not processed through Capita HR. Work is progressing, but BIS estimate that delivery of a solution will be 31 July 2012 at the earliest. |
| **Recommendation 3** | |
| Staff with system administrator level access or similar should be reviewed and verified on an annual basis. | |
| **Responsibility** | Capita (Ben Lindley) / SCC Finance (Julie Fletcher) |
| **Priority** | Low |
| **Date** | Annual Review in September 2011 |
| **2010/11 Authority Comments** | Action taken to remove non-required administrator level access. Next annual review scheduled for September 2011 will include engagement with SCC FSSG for Finance System specific controls and general procedures to ensure temporary administrator rights are based on immediate business need and time limited; and where identified as no longer required, removed in a timely manner. |
| **2011/12 Audit update** | This recommendation has been implemented. |
| **Recommendation 4** | |
| Network user accounts which have not been used for a significant period of time, for example, six months, should be disabled. | |
| **Responsibility** | Capita (Ben Lindley) |
| **Priority** | Medium (Initial)/Low (Process) |
| **Date** | Initial delivery for 31 March 2011/Process delivery in 2011/12 |
| **2010/11 Authority Comments** | Network User Accounts are regularly reviewed and appropriate action taken. This will be further supported by development of a policy and procedures for proactively managing dormant accounts, including disabling accounts with no activity for 90 days. |
| **2011/12 Audit update** | Our follow up work in December 2011 noted 333 accounts that had not been used between April and September 2011 and for which access was still available (i.e. they had not been disabled / deleted).<br>In February 2012, Council officers informed us that Capita had implemented this process, and it is now completed on a monthly basis.<br>We confirmed that the process was operating satisfactorily in May 2012. |

## Recommendations

### Recommendation 5

A formal monitoring or exception reporting system should be implemented to cover staff with remote access to key financial systems.

| | |
|---|---|
| **Responsibility** | SCC Finance (Eugene Walker/Julie Fletcher) / Capita (David Cunningham) |
| **Priority** | Medium (Initial) / Low (Process) |
| **Date** | Initial Review for 31 March 2011 / Policy/Process in 2011/12 |
| **2010/11 Authority Comments** | An initial review of Remote Access privileges for Finance System users will be undertaken in this financial year and appropriate 'cleansing' action implemented to remove unnecessary remote access accounts. Following this, a process for proactively managing the granting of Remote Access use in the specific context of Finance Systems will be developed jointly by SCC Finance Services Support Group (FSSG) and Capita. This process will include input on Security Policy issues from BIS Information Management. |
| **2011/12 Audit update** | The Council have responded stating they are reliant on Capita to advise FSSG when a user is granted remote access, as it is not possible to monitor this from within OEO. Officers within BIS remain satisfied that RAS is a secure system access medium and in their view there are no additional risks in users accessing OEO via this method.<br>Our view is the recommendation remains relevant particularly given that a large number of staff have remote access to the Council's financial systems, and given the potential increase in home and remote working over the next few years. Our judgement is that controls would be strengthened if formal procedures were developed and introduced to monitor staff accesses. These controls should look for unusual patterns of activity, for example staff persistently logging-in during the night or weekend, which in our experience can be indicators of issues occurring. However we recognise that there would be resource implications to implementing this recommendation. Consequently we suggest that officers should keep the position under review, balancing the risk against the costs of compliance. |

### Recommendation 6

The Council should request annually from all third party IT service providers an independent assurance statement that the general IT controls covering the main financial systems at their main data centres are operating effectively.

| | |
|---|---|
| **Responsibility** | SCC Finance (Eugene Walker/Julie Fletcher) / Capita (Pat Gee) |
| **Priority** | Medium (Initial)/Low (ongoing) |
| **Date** | Initial request/response for 31 March 2011 / Ongoing in 2011/12 |
| **2010/11 Authority Comments** | Capita provides information on ICT controls at data centres under its control. SCC Finance will initially request independent assurance statements from Finance System providers. |

| Recommendations | |
|---|---|
| | Following receipt and review of the responses, a process for requesting and receiving timely statements as to the efficiency of IT controls for Finance Systems across the Council's estate will be developed and implemented by SCC Finance with Capita input and support. |
| **2011/12 Audit update** | The Council has agreed that they have not yet sought assurances on the adequate operation of general IT controls from service providers. FSSG are to set a reminder to ask Velos to verify this annually. |

| Recommendation 7 | |
|---|---|
| The Council should agree a comprehensive business continuity and disaster recovery plan for the systems and services they receive from Capita including a level of priority. (Capita manages many clients; each will have agreed a different level of disaster recovery or order of priority to get their services restored in the event of a disaster). | |
| **Responsibility** | BIS (Ian Jellyman) |
| **Priority** | Medium (Initial)/Medium (Ongoing) |
| **Date** | Initial for 31 March 2011/Ongoing in 2011/12 |
| **2010/11 Authority Comments** | Initial - An assessment and report of the current status of business continuity and disaster recovery plans relating to the data centre; IT systems and Financial systems under Capita control.<br>Ongoing – A comprehensive review of business continuity and data centre disaster recovery plans; policies; procedures; including the relative status of Sheffield applications alongside contractual obligations of Capita to other contracts under their management. |
| **2011/12 Audit update** | The Council has made good progress in addressing the recommendation. Phase 1 Disaster Recovery testing is now complete for six systems with reports just requiring formal sign-off by the SIP Programme Board. Testing included systems, data and access via thick client in a model office in Sheffield.<br>Phase 2 testing is pending the completion of a major Citrix upgrade due for completion in May 2012. Update June 2012 - the recommendation is still agreed but this implementation has been delayed.<br>It is planned that Disaster Recovery testing across all systems will be done annually in future years. The Council needs to monitor to ensure this is done. |

| Recommendation 8 | |
|---|---|
| The Council should request the results of annual disaster recovery tests on the main financial systems they use. | |
| **Responsibility** | SCC Finance (Eugene Walker/Julie Fletcher) / BIS (Ian Jellyman) |
| **Priority** | Low |
| **Date** | Delivery within 2011/12. |

| | |
|---|---|
| **2010/11 Authority Comments** | A review of existing disaster recovery plans for Council systems, including verifying the validity of test results from such tests will be delivered.<br>Recommendations from the review along with all options for improvements in both policy and procedure will be shared with Stakeholders with the aim of creating an affordable, robust and reliable action plan for disaster recovery testing and validation of SCC Financial systems and supporting ICT infrastructure. |
| **2011/12 Audit update** | Refer to comments made within recommendation 7. |

# Appendix 2 - 2010/11 Report conclusion and key findings (included here for information)

**8** Overall, we have concluded your IT arrangements for the key financial systems present a low risk of material error in your 2010/11 accounts. In the main, there are good IT arrangements in place; however, we have identified some areas where there are control weaknesses, which we bring to your attention below.

## IT Entity level controls

**9** IT Entity level controls overall are satisfactory and there are no significant concerns in the following areas.

- Incident/Problem management.
- IT risk management.
- General network infrastructure control.
- IT policies and procedures.

**10** The only weak area noted is the absence of a formal Information Systems and/or Information Technology strategy. In our view, this is significant as the Council commenced a contract in January 2008 to outsource all ICT service delivery functions including HR/Payroll and Revenues/Benefits functions to Capita under a seven-year contract with options to extend to 13 years at approximately £15 million per year.

**11** A strategy should have been in place at the beginning of the outsourcing process to give the vision, clear objectives and implementation plan for the future including expected outcomes and expected benefits both quantitative and qualitative. In addition, it would have established a link to and show how the corporate objectives of the Council are supported.

| Recommendation |
| --- |
| **R1** A IS/IT strategy should be developed which clearly documents the way forward including the expected cash releasing savings and how the outsourced contract will be monitored and regularly reported to the Council. |

## Access security controls

**12** Overall, logical access control arrangements are assessed as weak with scope for improvement.

13 The main findings in this section are as follows.

- Weak arrangements for disabling staff leavers in a timely manner including the absence of a 'Leaver's checklist'. A sample of leavers were checked against records held with results ranging from a leaver account still active to several accounts disabled sometime after the users' departure date.
- A high number of system administrator level accounts were identified. Further investigation showed that some staff no longer required this level of access but had retained it. On raising the matter, action was immediately agreed to review and reduce the number of staff with this type of level of access.
- A report requesting the number of network user accounts not used for the period between 1 April – 30 September 2010 showed there are 611 active network accounts which had no recent activity. This is a potential security weakness and the Council may be incurring a maintenance or licence cost on network accounts which are dormant or rarely used.
- A report was requested to identify the number of staff with anytime remote access to Council IT systems. There are 1,106 users of which 451 have access to the main financial system and 373 of those can access the Qtier system. Mobile and home working is becoming a more accepted method of working; our main concern is the absence of a formal monitoring mechanism for staff using remote access.

## Recommendations

| | |
|---|---|
| **R2** | The procedure for the disabling the user accounts of staff leaving the employment of the Council should be re-designed to ensure it is more timely and complete. This should include a checklist to ensure all IT equipment is collected, for example, any two factor remote access devices, mobile devices and laptops. |
| **R3** | Staff with system administrator level access or similar should be reviewed and verified on an annual basis. |
| **R4** | Network user accounts which have not been used for a significant period of time, for example, six months, should be disabled. |
| **R5** | A formal monitoring or exception reporting system should be implemented to cover staff with remote access to key financial systems. |

## Data centre and network controls

**14** The Council has outsourced the operation and delivery of its main financial systems to third parties – Capita IT and Velos. We have received for the former a copy of a Certificate of Registration showing attainment of the Information Security Management System (ISMS) – ISO/IEC 27001:2005 security accreditation. No similar documentation for the latter was provided.

**15** ISMS is more a security accreditation than confirmation that general IT controls at the data centre(s) are operating correctly and effectively. Our IT risk assessment is directed towards providing assurance on the general IT control environment while the above is primarily one to give assurance on IT security.

**16** The Council does not routinely request any formal assurance on the adequacy of arrangements to deliver their IT service requirements. We therefore have no information on the adequacy of the general IT controls to support the operation of the main financial systems.

**17** The position on data backup cycles and test restores is overall satisfactory. The responses for confirmation that operating systems and application software were included were unclear and not verified.

**18** Recent evidence to show disaster recovery tests for both the Resourcelink payroll system and the main accounting system were provided by suppliers Northgate and Velos respectively. However, for all other application systems the Council does not presently have a fully tested IT disaster recovery arrangement with Capita. This could impact the ability to process and report on financial transactions in the event the main accounting and subsidiary financial systems are unavailable.

**19** The ISMS certificate does list that Capita has achieved a satisfactory level of business continuity and disaster recovery planning. However, this should be taken as evidence that it applies to Capita and that it does not automatically cover the Council's requirements or priorities.

**20** We are surprised that after two years into a contract where the Council has outsourced some key services, a firm disaster recovery plan and subsequent arrangements have not yet been implemented.

**21** We noted that there are some good controls for management of the network infrastructure and prevent unauthorised external access and protect data and systems from malicious software.

### Recommendations

**R6** The Council should request annually from all third party IT service providers an independent assurance statement that the general IT controls covering the main financial systems at their main data centres are operating effectively.

| Recommendations | |
|---|---|
| R7 | The Council should agree a comprehensive business continuity and disaster recovery plan for the systems and services they receive from Capita including a level of priority. (Capita manages many clients; each will have agreed a different level of disaster recovery or order of priority to get their services restored in the event of a disaster). |
| R8 | The Council should request the results of annual disaster recovery tests on the main financial systems they use. |

## Program change controls, new systems acquisition and development

22 The above were reviewed and noted as operating satisfactorily. No issues or significant risks identified.

## End user computing

23 The above were reviewed and noted as operating satisfactorily. No issues or significant risks identified.

If you require a copy of this document in an alternative format or in a language other than English, please call:
**0844 798 7070**


Design and production by the Audit Commission Publishing Team.


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.


Audit Commission

1st Floor
Millbank Tower
Millbank
London
SW1P 4HQ

Telephone: 0844 798 3131
Fax: 0844 798 2945
Textphone (minicom): 0844 798 2946

www.audit-commission.gov.uk June 2012