



GOVERNMENT

Interim Audit Report 2008/09

Leeds City Council

June 2009

AUDIT

The contacts at KPMG in connection with this report are:

Adrian Lythgo

Associate Partner
KPMG LLP (UK)

Tel: 0113 231 3054

Fax: 0113 231 3941

adrian.lythgo@kpmg.co.uk

Jillian Burrows

Senior Manager
KPMG LLP (UK)

Tel: 0161 246 4705

Fax: 0113 231 3941

jillian.burrows@kpmg.co.uk

Alison Ormston

Manager
KPMG LLP (UK)

Tel: 0113 231 3444

Fax: 0113 231 3941

alison.ormston@kpmg.co.uk

Sam Bradford

Assistant Manager
KPMG LLP (UK)

Tel: 0113 231 3624

Fax: 0113 231 3941

sam.bradford@kpmg.co.uk

Page

Executive summary

2

Financial statements

3

Appendices

6

- A. Recommendations arising from 2008/09 interim audit
- B. Follow up of prior year recommendations
- C. Accounts risks

This report is addressed to the Authority and has been prepared for the sole use of the Authority. We take no responsibility to any member of staff acting in their individual capacities, or to third parties. The Audit Commission has issued a document entitled Statement of Responsibilities of Auditors and Audited Bodies. This summarises where the responsibilities of auditors begin and end and what is expected from the audited body. We draw your attention to this document.

External auditors do not act as a substitute for the audited body's own responsibility for putting in place proper arrangements to ensure that public business is conducted in accordance with the law and proper standards, and that public money is safeguarded and properly accounted for, and used economically, efficiently and effectively.

If you have any concerns or are dissatisfied with any part of KPMG's work, in the first instance you should contact Adrian Lythgo, who is the engagement Associate Partner to the Authority, telephone 0113 231 3054, email adrian.lythgo@kpmg.co.uk who will try to resolve your complaint.

If you are dissatisfied with your response please contact Trevor Rees on 0161 236 4000, email trevor.rees@kpmg.co.uk, who is the national contact partner for all of KPMG's work with the Audit Commission. After this, if you are still dissatisfied with how your complaint has been handled you can access the Audit Commission's complaints procedure. Put your complaint in writing to the Complaints Investigation Officer, Westward House, Lime Kiln Close, Stoke Gifford, Bristol, BS34 8SR or by e mail to: complaints@audit-commission.gov.uk. Their telephone number is 0844 798 3131, textphone (minicom) 020 7630 0421

Executive summary

Scope of this report

This report summarises our planning and interim audit work at Leeds City Council ('the Authority') in relation to the 2008/09 financial statements. A significant proportion of our accounts audit is completed before we receive your financial statements. In particular, our work to date covers the following areas:

- Audit planning and risk analysis: We have identified the key issues for the 2008/09 financial statements and discussed your progress in addressing these.
- Control evaluation: We have reviewed your progress with the closedown and accounts production process. We have also tested controls over the key financial systems. We rely on the work of internal audit wherever possible, and complete an assessment of the internal audit function as part of this work.

Section 2 provides further details of the work completed and sets out our findings.

Our recommendations arising from our 2008/09 interim audit are included in Appendix A. We have also reviewed your progress in implementing prior recommendations and this is detailed in Appendix B.

This is the first year that we have presented a formal report to the Audit Committee. In prior years we have presented an informal report to management highlighting our planning and interim audit findings. However given that one of the recommendations, relating to establishment checklists raised in prior years has not been satisfactorily resolved the decision has been made, and agreed with Doug Meeson, to present a formal report to the Audit Committee summarising the results of our planning and interim audit work.

Summary of findings

- The Authority's accounts production process is planned appropriately;
- The Authority has taken steps to address the specific audit risks we have identified;
- Our review of the Authority's entity level controls found no issues at this stage;
- Our review of the Authority's IT general controls found two issues in respect of user access to financial systems which are discussed in more detail in this report;
- Our review of the high level controls for the key financial systems found one issue concerning payroll establishment checklists which is discussed in more detail in this report. The exact details of the impact that this may have on our final audit is still being determined and will be reported within the 2008/09 ISA 260 report; and
- Our review of internal audit found the operation of Internal Audit to be good, we were able to place reliance on work covered by internal audit on the key financial systems and sample sizes used by internal audit were sufficient for our purposes.

Acknowledgements

We would like to take this opportunity to thank officers and members for their continuing help and co-operation throughout our audit work.

Financial statements

Introduction

Our work in respect of the audit of financial statements is split into four stages as shown below:

| Stage | Tasks | Timing | Completed |
|---------------------|--|--------------------------------|-----------|
| Planning | <ul style="list-style-type: none"> Updating our business understanding and risk assessment Assessing the organisational control environment Issuing our accounts audit protocol | December 2008 to February 2009 | ✓ |
| Control Evaluation | <ul style="list-style-type: none"> Reviewing the accounts production process Evaluating and testing controls over key financial systems Review of internal audit | March to April 2009 | ✓ |
| Substantive Testing | <ul style="list-style-type: none"> Planning and performing substantive work Concluding on critical accounting matters | July to August 2009 | - |
| Completion | <ul style="list-style-type: none"> Completion procedures Forming our audit opinion | September 2009 | - |

Key issues in respect of each of these tasks is summarised below.

Planning - Risk assessment

Our 2008/09 *Audit and Inspection Plan*, presented to you in June 2008, included our initial assessment of the risks impacting on the 2008/09 financial statements. We have updated this and consider the following areas to be the key accounting issues for 2008/09.

- Compliance with the 2008 *Statement of Recommended Practice on Local Authority Accounting the UK* (SORP): includes a number of changes, including prohibiting the revaluation of fixed assets on disposal and introducing the concept of 'revenue expenditure funded from capital under statute'.
- Accounting estimates and valuations: The current economic environment introduces a number of risks for the financial statements, in particular for estimates and valuations. This includes the valuation of fixed assets which are carried at market value (such as investment properties and surplus assets) and the assessment of recoverability of debts to determine appropriate provisions.
- Minimum Revenue Provision: In the past all capital expenditure has been treated the same when calculating the Minimum Revenue Provision (MRP). The *Local Authorities (Capital Finance and Accounting) (England) (Amendment) Regulations 2008* now require authorities to make a 'prudent' provision. The Authority approved its MRP policy in February 2009 and will be basing the 2008/09 MRP on asset lives. This is more complex than the methodology adopted previously and requires accurate fixed asset information.

We will continue to discuss these risks with your finance team as part of our regular meetings with them.

You have taken our audit risks seriously and made progress in addressing the risks identified. However, these still present significant challenges that require careful management and focus. We will revisit these areas during our final accounts audit.

Further details are included in Appendix C, which also provides a summary of work you have completed to date to address these risks.

Financial statements (continued)

Planning - Organisational control environment

Most of the organisational controls we assess are linked to our use of resources work, which also considers your system of internal control.

We consider that your organisational controls are effective overall.

We also consider controls over the use of information technology (IT).

We found that you have further strengthened your IT control environment but noted continuing weaknesses (which are highlighted in Appendix A) :

- There is no formal process in place for monitoring access to FAB and Academy. i.e. reviewing personnel that have access to these systems and whether their access rights are inline with their job role.
- FAB - There is a weakness where a system administrator responsible for issuing passwords could issue a password to themselves as an infrequent user in order to access FAB. Whilst infrequent user accounts become inactive after 3 months there is still a risk that should an individual wish unauthorised changes could be made.

Planning - Accounts audit protocol

This important document explains our audit process with details of our audit team, audit approach and timetable. It also summarises the working papers and other evidence we require you to provide as part of the preparation of the financial statements. We issued this to Chris Blythe and discussed this as part of our final accounts planning meeting. We have tailored the document to reflect our requirements in respect of the specific accounting issues identified above.

Control Evaluation - Accounts production process

We have reviewed your plans for preparing for your closedown and accounts preparation. You have incorporated a number of measures into your closedown plan to further improve the project management of this complex process.

We consider that your process for the preparation of your financial statements are good, this was reflected in the 2008 Use of Resources score of a level four.

Financial statements (continued)

Control Evaluation - Controls over key financial systems

We work with internal audit to:

- update our understanding of key financial systems;
- confirm our understanding of these systems by completing walkthrough testing; and
- document, evaluate and test the control framework for these systems.

We rely on any relevant work internal audit have completed for 2008/09. For each of the key financial systems, they tested the high level controls that we would expect to be in place. High level controls are strong controls that should address the key risks. Examples are reconciliations or exception reports.

We assessed your high level control framework as satisfactory overall but noted some weaknesses in respect of the following individual financial system:

- Establishment Checklist: During our testing we found that establishment checklists are not being completed across the Council. A pilot was undertaken within the resources department of undertaking establishment checklists and managers found a relatively large number of adjustments were necessary to the payroll system.

We have not yet assessed the controls over fixed assets and financial reporting. Many of the high level controls in respect of these areas are operated during the closedown process and our testing will be supplemented by further work during our final accounts visit.

Control Evaluation - Review of internal audit

The *Accounts and Audit Regulations 2003* require public bodies to maintain an adequate and effective system of internal audit of their accounting records and of their system of internal control. For principal local authorities, guidance is contained in the *Code of Practice for Internal Audit in Local Government* ('the Code'). The Code defines the way in which internal audit should be established and operated and applies equally to in-house audit teams and those provided by external contractors.

We did not identify any significant issues with their work and are pleased to report that we have again been able to place full reliance on internal audit's work on the key financial systems. We particularly noted improvements in terms of the adequacy of sample sizes used by internal audit.

There was, however, one area where some improvements could be made to further enhance the quality of internal audit's work and reduce the level of top up testing we are required to complete to satisfy our audit requirements, including:

- As part of our testing on Payroll if the establishment checklists are not in place we are required to look at the controls in place over the addition, amendment and deletion of staff from the payroll system. This year it was necessary for us to complete further top-up testing as the sample sizes used by internal audit were not sufficient for our purposes.



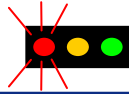
**Appendix A:
Recommendations
arising from 2008/09
interim audit**

Appendix A: Recommendations arising from 2008/09 interim audit

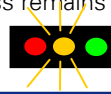
We have given each recommendation a risk rating (as explained below) and agreed what action management will need to take. We will follow up these recommendations next year.

Priority rating for recommendation

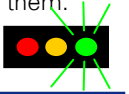
Priority one: issues that are fundamental and material to your system of internal control. We believe that these issues might mean that you do not meet a system objective or reduce (mitigate) a risk.



Priority two: issues that have an important effect on internal controls but do not need immediate action. You may still meet a system objective in full or in part or reduce (mitigate) a risk adequately but the weakness remains in the system.




Priority three: issues that would, if corrected, improve the internal control in general but are not vital to the overall system. These are generally issues of best practice that we feel would benefit you if you introduced them.



| No. | Risk | Issue and recommendation | Management response | Officer and due date |
|-----|------|---|---|---|
| 1 | | <p>Establishment Lists and Payroll Amendments.</p> <p>During our testing we found that establishment checklists are not being completed across the Council.</p> <p>A pilot was undertaken within the resources department of undertaking establishment checklists and managers found a relatively large number of adjustments were necessary to the payroll system.</p> <p>We have reviewed a sample of the adjustments that were necessary to the payroll system to ascertain the reasons for these. Based on the sample of our review the adjustments required did not affect the financial data within the payroll system.</p> <p>This pilot was only conducted within the resources directorate however, so there may be departments which are higher risk where they have high staff turnover.</p> <p>We would therefore recommend that the Council continue to utilise the high level control of establishment checklists to gain assurance over the data held within the payroll system.</p> <p>Whilst we understand that management are of the opinion that undertaking establishment checklists in the format undertaken within the pilot are an onerous administrative burden we understand that management are looking at alternative controls to address this.</p> | <p>Although there is currently no formal system for monitoring establishments straight from SAP there are a number of controls in place to ensure establishment lists are correct:</p> <ul style="list-style-type: none"> • All schools undertake regular detailed establishment checks, monitored by Education Leeds. • Monthly budget monitoring of payroll costs including, in many instances, the use of a direct download from SAP. • Managers receive payslips which would indicate if officers had left the authority but had still been paid (only 3,307 officers have their payslip sent directly to their homes out of an establishment of some 33,000). • SAP Managers Desk Top facilities have been rolled out to 65 managers to enable officers to undertake their own establishment checks straight from SAP, rather than relying on check lists produced by BSC. • Acting up and honoraria checks in place, including end dates and extension confirmation requirements. <p>In addition to the above the following actions are to be implemented:</p> <ul style="list-style-type: none"> • Business case is being developed for the purchase of the SAP Managers Self Service module. This module will allow managers to access all establishment details. • Further roll out of another 40 of the current SAP Management Desk Top to high risk areas identified in Youth Services & Early Years. | <p>Chief Officer Business Support Centre And Head of Finance Corporate Financial Management</p> <p>MSS business case to be completed by Aug 2009. 83 further managers desk tops to be rolled out by July 2009. Review of budgetary controls on establishment lists to be completed by September 2009.</p> |

Appendix A: Recommendations arising from 2008/09 interim audit (continued)

| No. | Risk | Issue and recommendation | Management response | Officer and due date |
|-----|---|--|---|--|
| | | <ul style="list-style-type: none"> | <ul style="list-style-type: none"> • BSC currently investigating alternative method of producing establishment lists using graphical structure charts made available via a secure area on the intranet, which will simplify the checking process for Managers and reduce the administrative burden. • HR officers in each Directorate have been charged with ensuring establishment lists are up to date. • Review of the budget monitoring arrangements to ensure appropriate checks are made on establishment lists. | |
| 2 |  | <p>IT – General Ledger Controls</p> <p>There is no formal process in place for monitoring access to the General Ledger (FAB) and Academy. i.e. reviewing personnel that have access to these systems and whether their access rights are inline with their job role.</p> <p>There is a risk that the system administrators (eight staff who are based within central finance) who work with the General Ledger (FAB) also have the ability to amend their access permissions and thus bypass the controls enforced to segregate roles and responsibilities within the department.</p> <p>Without a formal process in place for monitoring access rights there is a risk that users may end up with inappropriate access right due to changes in their job role.</p> <p>We recommend for both issues that a monitoring process is implemented that covers all users including super users and system administrators to ensure that access levels are appropriate and the users are still required to have access to the system. This should be performed on a regular basis (at least quarterly). The monitoring should be formal and signed-off</p> | <p>Current controls (FAB):</p> <ul style="list-style-type: none"> • A list of all leavers received via ICT and access removed by system controllers. • Access rights reviewed when officers move between directorates. System controllers can only give access rights within their own Directorates. • Chief Officers approve officers payment authorisation rights. Officers who can authorise payments cannot raise orders. • All transactions traceable to the users ID. • Responsibility of system controllers to ensure access rights are up to date. Responsibility covered in training given to all system controllers. • ICT and Financial Development have a small number of users who can amend anyone's rights but they cannot issue passwords. <p>Only a limited number of staff within Corporate Financial Management can amend access rights, set up new users and amend passwords. As in any system someone must have the power to set passwords. The FMS module allowing this level of control is itself password protected. The password automatically expires after 40 days and is changed whenever the officers with these access rights move on.</p> <p>Agreed that the Principal Accountant (CFM) will monitor these high level access rights on a monthly basis. The monitoring will include the appropriateness of access rights and that regular password changes are undertaken.</p> | <p>Principal Accountant Corporate Financial Management.</p> <p>Due date: 1st quarter 2009/10.</p> |

Appendix A: Recommendations arising from 2008/09 interim audit (continued)

| No. | Risk | Issue and recommendation | Management response | Officer and due date |
|--------------|------|--------------------------|---|--|
| 2 (contd) | | | <p>Current controls (Academy):</p> <p>Each officer receiving access is reminded of the security protocols.</p> <p>There is an audit trail for all updates to the system.</p> <p>Unit managers revoke permissions for staff leaving the service. This is backed up by the Business Continuity Team.</p> <p>Officers requesting access outside the service are required to get agreement of their section head and provide a business case. Access outside the service is limited to view only.</p> <p>Anyone whose access hasn't been used for 3 months has their access revoked.</p> <p>Passwords automatically expire after 40 days.</p> <p>17 officers have permissions to change passwords. There is an audit trail which identifies who has updated the permissions or changed a password. In addition a systems event log is kept of all changes.</p> <p>Agreed that senior officers within the Business Continuity Unit will undertake random checks on password changes where the person has update access (rather than view only). The monitoring will also review whether the list of officers with powers to amend passwords is up to date. This monitoring will be completed on a monthly basis.</p> | <p>Officer: Executive Officer, Policy & Finance, Leeds Benefits Service.</p> <p>Due date: 1st quarter 2009/10.</p> |



**Appendix B:
Follow up of prior
year
recommendations**


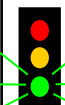
Appendix B: Follow up of prior year recommendations

This appendix summarises the progress made to implement the recommendations identified in our previous reports.

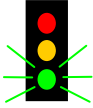
| Report | Number of recommendations that were: | | |
|------------------------------|--------------------------------------|-----------------------------------|--|
| | Included in original report | Implemented in year or superseded | Remain outstanding (re-iterated below) |
| Interim Audit Report 2007/08 | 7 | 3 | 4 |
| Total | 7 | 3 | 4 |

| No. | Risk | Issue and recommendation | Management response | Officer and due date | Status at 9 April 2009 |
|-----|------|--------------------------|---------------------|----------------------|------------------------|
|-----|------|--------------------------|---------------------|----------------------|------------------------|


Interim Audit Report 2007/08

| | | | | | |
|---|---|--|---|-----------|---|
| 1 |  | <p>Establishment Lists</p> <p>We have raised this issue in our 2006/07 interim report. During our work at the Council we identified that although establishment reports are produced there is no evidence that these reports are being reviewed.</p> <p>The Council are aware of this and have plans in place to ensure that this evidence will be in place in future years and there will be a central record of those departments which are complying with the need to review their establishment lists.</p> <p>Teachers payroll establishment reports are sent and returned on a monthly basis to evidence their review.</p> | A pilot is to be undertaken within the resources department relating to the production and review of paper based exception reports. | 2008/09 | <p>Not implemented</p> <p>A pilot was undertaken in 2008/09 for the production and review of paper based exception reports within the resources directorate.</p> <p>The pilot exercise undertaken highlighted that his was a large administrative burden and management are currently looking at alternative controls to address this.</p> <p>This is detailed in our report above.</p> |
| 2 |  | <p>Exception reports</p> <p>Currently the Council produce a comprehensive range of exception reports for the payroll system.</p> <p>Team leaders within payroll are required to review the exceptions listed on the report and show their agreement or otherwise by returning the report to payroll.</p> <p>We found that there is some inconsistency and returns are not always made to confirm that all action points raised by exception reports have been investigated and appropriate action taken.</p> <p>This is a control weakness we identified in our 2006/07 interim visit.</p> | Agreed | Immediate | <p>Implemented</p> <p>The high level signing off of these exception reports is now occurring.</p> |

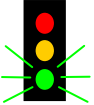
Appendix B: Follow up of prior year recommendations (continued)

| No. | Risk | Issue and recommendation | Management response | Officer and due date | Status at 9 April 2009 |
|-----|---|--|--|----------------------|---|
| 3 |  | <p>Powersolve Debtors Reconciliation</p> <p>A sample of two of the above reconciliations were reviewed in detail during our interim visit. Through this review it was identified that there were items on the reconciliation marked as 'items under investigation'. As a result we reviewed all of the reconciliations performed, which was up to the end of February. Each reconciliation has a varying amount marked as this each month with the amounts being less than £1000. We understand that the description on the reconciliation is misleading as the balance represents timing differences between the reporting of the two systems, not unidentified differences. We also understand that individual transactions on each system are reconciled each month. We recommend that the council should review the reporting arrangements for the systems to investigate why the timing differences occur and how these can be eliminated.</p> <p>This is an issue we identified in both our 2005/06 & 2006/07 interim audit visits.</p> | <p>The Council have undertaken an exercise to identify the causes of the small difference (£133.21) and have identified that this is a historical error going back to the earliest set of records that the Council have. It has therefore been agreed to write this off.</p> | <p>March 2009</p> | <p>Implemented</p> <p>This balance has been investigated by they Council and it has been written off.</p> |

Appendix B: Follow up of prior year recommendations (continued)

| No. | Risk | Issue and recommendation | Management response | Officer and due date | Status at 9 April 2009 |
|----------------------------------|---|---|--|---|------------------------------------|
| IT interim report 2007/08 | | | | | |
| 1 |  | <p>IT Security Policy</p> <p>Although Leeds City Council has a detailed Information Security Policy staff are not required to read and understand the Information Security Manual when they join the organisation. There is no continuous Security Awareness program in place presently, though this is planned for implementation later this year in order to comply with some specific projects across the authority.</p> <p>The IT Security Policy should be formally distributed to all staff and locations. Internal audit department should ensure that all staff follow the procedures defined in the policy.</p> <p>The benefit will be that end-users should be aware of their roles and responsibilities with respect to access to programs and data, which includes an understanding of the risk of sharing passwords or downloading unauthorized programs or files (e.g. from the internet). Improvements in Information Security knowledge sharing will provide greater assurance that persons understand the risks associated with critical information.</p> | <p>As part of the Council's move to use Government Connect to access DWP services for benefits we are required to formalise the induction process for all new staff and have a refresher during the course of a person's employment.</p> <p>We are working with HR to ensure a common approach across the council to meet this requirement.</p> <p>The target is for this to be complete and embedded by Sept 2009. This date is a requirement for access to DWP services so it's not moving and we are confident that we'll hit it.</p> | <p>September 2009</p> <p>Adrian Fegan Head of ICT Service Delivery.</p> | <p>As per management response.</p> |


Appendix B: Follow up of prior year recommendations (continued)

| No. | Risk | Issue and recommendation | Management response | Officer and due date | Status at 9 April 2009 |
|-----|---|---|---|--|------------------------|
| 2 |  | <p>Physical Access</p> <p>We noted that the removal of proximity and magnetic stripe cards used for access to various Leeds CC sites and data server rooms is not properly controlled. Currently the removal of such cards is based on information provided by a line manager at the time an employee leaves the organisation. Auditing of access is not performed to regularly to ensure physical access is appropriately controlled for both full time employees and contractors.</p> <p>Absence of adequate physical access controls results in a high level of risk for Leeds City Council in the form of unauthorised access to the building and sensitive information. Critical IT equipment housed in the Datacentre could be damaged or stolen resulting in disruption of operations. Inadequately controlled access to the Datacentres exposes the systems to unauthorised access by users increasing the risk of wanton or accidental damage to the servers or other key IT equipment.</p> <p>We recommend that the Network Management Team (NMT) should always be informed by a line manager or HR should an employee or contractor leave the organisation. In addition, periodic reviews of physical access should be performed to ensure the access to facilities is appropriately controlled.</p> <p>The improvement in the above control will provide greater assurance that the Council is not susceptible to reputational damage or regulatory fines.</p> | <p>ICT has a controlled process in place to ensure access to data centres and other primary ICT sites is managed. All primary sites are now linked into a single system that requires a proximity card and pin to access.</p> <p>These cards are centrally controlled within ICT. Authorised staff lists are maintained by two methods. Firstly a monthly report from SAP is produced that includes all leavers from ICT.</p> <p>Secondly all leavers within ICT are reported from ICT admin staff on a weekly report to the access control team. The leaving process includes returning access cards, equipment, etc back into admin</p> | <p>2008/09</p> <p>Adrian Fegan Head of ICT Service Delivery.</p> | <p>Implemented.</p> |

Appendix B: Follow up of prior year recommendations (continued)

| No. | Risk | Issue and recommendation | Management response | Officer and due date | Status at 9 April 2009 |
|-----|---|--|--|--|-----------------------------------|
| 3 |  | <p>Access to applications</p> <p>Users can access a number of applications and financial systems through the desktop. When a person leaves, HR inform ICT who then remove the desktop access.</p> <p>However user accounts to individual applications such as SAP, Academy and Powersolve are not always removed once a user ceases employment at the Council. We were informed that occasionally an email from a line manager informs SAP administrators that a user has left. A monthly report run on SAP identifies accounts which have not been used for 3 months. ICT team disable accounts which have not been used based on this output. It was noted that accounts are remaining active to facilitate new users who replace the original account owners.</p> <p>There is a risk that another person may use the accounts of persons leaving the organisation, if not deleted and disabled promptly, to gain access to the individual application exposing the council to risk of fraudulent unaccountable access.</p> <p>ICT should ensure that all application accounts (as well as desktop access) are deleted and disabled when either a permanent or temporary employee leaves the council. The system administrator should delete the ID promptly and not just disabled when the employee leaves.</p> <p>The improvement in the above control will provide greater assurance that the council is not susceptible to reputational damage or regulatory fines.</p> | <p>When a person leaves the Council a flag is set within SAP that flags an account for deletion. This process is automatic and accounts are disabled once notification is received by the ICT Account Management Team.</p> <p>The first action is to disable the persons Novell account. This account is the primary account for all staff and is required to access the network before any other services.</p> <p>The account is then deleted after 30 days. We choose to disable and delete this is to enable access back to corporate information that might have been stored in the individual's account. We are also working with primary application owners to flag accounts that should be retired. The process will be managed via our request management system, Remedy, to enable the process to be workflowed and tracked. This work is progressing through Q1 2009. A target completion date will be set in Q1</p> | <p>June 2009</p> <p>Adrian Fegan Head of ICT Service Delivery.</p> | <p>As per management response</p> |

Appendix B: Follow up of prior year recommendations (continued)

| No. | Risk | Issue and recommendation | Management response | Officer and due date | Status at 9 April 2009 |
|-----|---|---|--|---|-----------------------------------|
| 4 |  | <p>Network level Access configuration</p> <p>We have noted that although SAP is used as the authoritative source of information for network level access administration and full time members of staff are removed from the network based on this information, temporary accounts are not administered this way.</p> <p>Temporary accounts (T-Accounts) are requested by line managers and are administered separately and bypass the controls enforced by using SAP. We understand requests have already been forwarded to the ICT team for account extensions from personnel acting as a previous user.</p> <p>The risk is that due to the number of T-Accounts and the lack of accountability and control over their creation and deletion there is a high risk of unauthorised access to the network. The situation arises where T-accounts are shared among temporary users to lessen the administration involved in setting up new accounts.</p> <p>We recommend that HR and ICT develop a procedure to keep track of the temporary staff and their use of T-accounts. In addition line managers should be reminded of their responsibilities to request and close t-accounts on a timely basis and separately for individual users.</p> | <p>Temporary accounts are not allowed under Government Connect and will be removed from use within the Council during 2009. It is worth noting that all T accounts are set for automatic expiry on creation.</p> | <p>December 2009 Adrian Fegan Head of ICT Service Delivery.</p> | <p>As per management response</p> |



Appendix C: Accounts risks

Appendix C: Accounts risks

This appendix summarises the key accounting issues for the 2008/09 financial statements and the progress you have made to date to address these.

| Issue | Risk and implications | Progress |
|--|--|--|
| <p>Compliance with the 2008 Statement of Recommended Practice on Local Authority Accounting the UK (SORP)</p> <p>The new SORP includes a number of changes, including prohibiting the revaluation of fixed assets on disposal and introducing the concept of 'revenue expenditure funded from capital under statute'.</p> | <p>There is a risk that the accounting for disposals has been treated incorrectly.</p> | <p>This is to be reviewed during the final audit visit.</p> |
| <p>Accounting estimates and valuations</p> <p>The current economic environment introduces a number of risks for the financial statements, in particular for estimates and valuations. This includes the valuation of fixed assets which are carried at market value (such as investment properties and surplus assets) and the assessment of recoverability of debts to determine appropriate provisions.</p> | <p>There is a risk that assets will be overvalued in the accounts and an adjustment is required having a detrimental effect on the net cost of services.</p> | <p>Information from the relevant systems has been obtained in order that the authority can make an accurate assessment of bad debt.</p> <p>In addition the valuer's and year end processes have been set up to identify any impairment issues,</p> |
| <p>Minimum Revenue Provision</p> <p>In the past all capital expenditure has been treated the same when calculating the Minimum Revenue Provision (MRP). The <i>Local Authorities (Capital Finance and Accounting) (England) (Amendment) Regulations 2008</i> now require authorities to make a 'prudent' provision.</p> | <p>There is a risk that MRP is miscalculated in the year.</p> | <p>The authority approved its MRP policy in February 2009 and will be basing the 2008/09 MRP on asset lives. This is more complex than the methodology adopted previously and requires accurate fixed asset information.</p> |
| <p>Reduction in Capital Receipts and Interest Rates</p> <p>Due to the recession and credit crunch Leeds City Council and other Local Authorities have experienced a reduction in the number and value of capital receipts which are used to fund the Council's capital program.</p> <p>In addition to this there has been a decrease in the interest rates which will affect the Council's lending and borrowing.</p> | <p>There is a risk that the level of capital receipts and interest is misreported and that the capital programme becomes unfeasible this could impact on cash flow, and treasury management arrangements</p> | <p>The Authority has scaled back the capital programme and put a number of schemes 'in reserve'. In addition the Authority have been looking at the process of assessing the financial viability of their key partners.</p> |