



*cutting through complexity™*

# Interim Audit Report 2011/12

Rotherham Metropolitan Borough Council

12 April 2012



**The contacts at KPMG in connection with this report are:**

**Stephen Clark**

*Director*

*KPMG LLP (UK)*

Tel: 0113 231 3148  
stephen.clark@kpmg.co.uk

**Rashpal Khangura**

*Senior Manager*

*KPMG LLP (UK)*

Tel: 0113 231 3396  
rashpal.khangura@kpmg.co.uk

**Amy Warner**

*Assistant Manager*

*KPMG LLP (UK)*

Tel: 0113 231 3089  
amy.warner@kpmg.co.uk

**Page**

**Report sections**

■ Introduction	2
■ Headlines	3
■ Financial statements	4
■ VFM conclusion	11

**Appendices**

1. Key issues and recommendations	14
2. Follow-up of prior year recommendations	18

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 which is available on the Audit Commission's website at [www.auditcommission.gov.uk](http://www.auditcommission.gov.uk).

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 Steve Clark, the appointed engagement lead to the Authority, who will try to resolve your complaint. If you are dissatisfied with your response please contact Trevor Rees on 0161 246 4000, or by email to [trevor.rees@kpmg.co.uk](mailto: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 Unit Manager, Audit Commission, Westward House, Lime Kiln Close, Stoke Gifford, Bristol, BS34 8SR or by email to [complaints@audit-commission.gov.uk](mailto:complaints@audit-commission.gov.uk). Their telephone number is 0844 798 3131, textphone (minicom) 020 7630 0421.

This document summarises the key findings arising from our work to date in relation to both the audit of the Authority's 2011/12 financial statements and the 2011/12 VFM conclusion.

### Scope of this report

This report summarises the key findings arising from:

- our interim audit work at Rotherham Metropolitan Borough Council (the Authority) in relation to the 2011/12 financial statements; and
- our work to support our 2011/12 value for money (VFM) conclusion up to March 2012.

### Financial statements

Our *External Audit Plan 2011/12*, presented to you in March 2012, set out the four stages of our financial statements audit process.



During January to March 2012 we completed our planning and control evaluation work. This covered our:

- review of the Authority's general control environment, including the Authority's IT systems;
- testing of certain controls over the Authority's key financial systems with the help of internal audit;
- high level assessment of the internal audit function; and
- review of the Authority's accounts production process, including work to address prior year audit recommendations and the specific risk areas we have identified for this year.

### VFM conclusion

Our *External Audit Plan 2011/12* explained our risk-based approach to VFM work, which follows guidance provided by the Audit Commission. We have completed some early work to support our 2011/12 VFM conclusion. This included:

- assessing the potential VFM risks and identifying the residual audit risks for our VFM conclusion;
- considering the results of any relevant work by the Authority, the Audit Commission, other inspectorates and review agencies in relation to these risk areas; and
- identifying what additional risk-based work we will need to complete.

### Structure of this report

This report is structured as follows:

- Section 2 summarises the headline messages.
- Section 3 sets out our key findings from our interim audit work in relation to the 2011/12 financial statements.
- Section 4 outlines our key findings from our work on the VFM conclusion.

Our recommendations are included in Appendix 1. We have also reviewed your progress in implementing prior year recommendations and this is detailed in Appendix 2.

### Acknowledgements

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

This table summarises the headline messages. The remainder of this report provides further details on each area.

Organisational and IT control environment	The IT control environment is effective overall and there has been progress since our review of the IT control environment in previous years. However we have identified areas for improvement over the access controls supporting a number of the key financial systems.
Controls over key financial systems	Controls around key financial systems have again been assessed as good. Audit work is still required around grant expenditure, capital, benefit expenditure and payroll expenditure, but these are predominantly year end controls and as such will be tested during our year end visit.
Review of internal audit	We have reviewed internal audit's work, and found it consistent with the Code of Practice for Internal Audit in Local Government. We were able to rely on their work for the majority of our interim controls testing, and found their working papers to have further improved from the good standard in prior years.
Updates to Code of Practice and other accounting issues	<p>There have been some updates to the Code of Practice for Local Authority Accounting for the 2011/12 year. These include :</p> <ul style="list-style-type: none"> <li>• Adopting the requirements of FRS30, Heritage Assets;</li> <li>• Amending the related party disclosures required and providing more guidance on the definition of a related party;</li> <li>• Additional guidance on accounting for:             <ul style="list-style-type: none"> <li>-- Pension strain;</li> <li>-- Grants and contributions; and</li> <li>-- the Carbon Reduction Commitment Scheme.</li> </ul> </li> </ul> <p>The Authority has been proactive in dealing with these issues and is making good progress in implementing any changes that are required.</p> <p>There are also on-going discussions around the accounting treatment for transactions related to RBT and Digital Region Ltd. Again, the Authority has been proactive in identifying and addressing the accounting issues.</p>
Financial resilience	<p>The Authority is still facing cost pressures, however the revised forecast overspend for the year had reduced to £3.066m (1.4%) at the time of writing this report. The Authority has also approved its budget for 2012/13, which included the cost savings required as a result of the funding cuts announced in the comprehensive spending review.</p> <p>The Authority continues to monitor its financial position and look at ways to reduce the forecast overspend.</p>
Other VFM risks	Our risk assessment identified value for money risks in relation to RBT and Digital Region Ltd. We will be undertaking work in relation to the arrangements to secure economy, efficiency and effectiveness in respect of these two issues prior to issuing our value for money conclusion.

Your organisational control environment is effective overall.

### Work completed

Controls operated at an organisational level often have an impact on controls at an operational level and if there were weaknesses this would have implications for our audit.

In previous years we used our work on the Use of Resources assessment to inform our findings in these areas. Due to the reduced scope of the VFM assessment we have to complete more specific work to support our financial statements opinion.

We obtain an understanding of the Authority's overall control environment and determine if appropriate controls have been implemented. We do not complete detailed testing of these controls.

### Key findings

In assessing the organisational control environment, we look at areas such as the Authority's response to political, economic and social factors, along with how they deal with any changes in accounting guidance. The Authority is always proactive in the management of any issues, and have good controls at an organisational level.

We therefore consider that your organisational controls are effective overall.

Aspect	Assessment
Organisational structure	3
Integrity and ethical values	3
Philosophy and operating style	3
Participation of those charged with governance	3
Human resource policies and practices	3
Risk assessment process	3
Information systems relevant to financial reporting	3
Communication	3
Monitoring	3

- Key:
- 1 Significant gaps in the control environment.
  - 2 Deficiencies in respect of individual controls.
  - 3 Generally sound control environment.

Your IT control environment is effective overall.

We noted a number of areas for further improvement.

- Process for removing leavers
- Improving password parameters
- Control over the use of user accounts assigned privileges
- Monitoring of the validity and appropriateness of access to users

### Work completed

The Authority relies on information technology (IT) to support both financial reporting and internal control processes. In order to satisfy ourselves that we can rely on the use of IT, we test controls over access to systems and data, system changes, system development and computer operations.

Testing of these areas has been completed by our IT audit specialists, focussing on the IT controls supporting the key financial systems.

### Key findings

We found your IT control environment is effective overall. We noted a number of areas for further improvement.

#### Leavers

- We noted that on both Cedar Financials and ICON Cash Receipting a number of user accounts for leavers had not been removed, thus increasing the risk of unauthorised access to key financial systems.

#### Password parameters

- We noted that the password minimum length and password history for Cedar Financials and ICON Cash Receipting and password history for PSe HR/Payroll were not set to best practice guidance.

#### Privileged User Accounts

- We noted that a generic privileged user account was still active on ICON following the recent upgrade of this system.
- We noted that privileged user accounts for Northgate Revenues & Benefits were set to have un-expiring passwords.
- Although it is acknowledged that some shipped privileged user accounts are used for batch/system jobs and password expiry

settings would result in key jobs failing, users should not have access to such accounts for day to day activities. In addition, access to privileged responsibilities should be supported by accounts that have password expiry.

#### Monitoring

- We noted that monitoring of user access to ICON, Northgate and PSe was limited in effectiveness, due to the lack of a clear strategy for monitoring, the reporting from the system for the purposes of subsequent monitoring or the lack of evidence of monitoring undertaken.

Recommendations are included in Appendix 1.

Aspect	Assessment
Access to systems and data	2
System changes and maintenance	3
Development of new systems and applications	3
Computer operations, incl. processing and backup	3

- Key:
- 1 Significant gaps in the control environment.
  - 2 Deficiencies in respect of individual controls.
  - 3 Generally sound control environment.



The controls over all of the key financial system are sound.

### Work completed

We work with your internal auditors to update our understanding of the Authority's key financial processes where these are relevant to our final accounts audit. We confirm our understanding by completing walkthroughs for these systems.

We then test selected controls that address key risks within these systems. The strength of the control framework informs the substantive testing we complete during our final accounts visit.

Our assessment of a key system will not always be in line with the internal auditors' opinion on that system. This is because we are solely interested in whether our audit risks are mitigated through effective controls, i.e. whether the system is likely to produce materially reliable figures for inclusion in the financial statements.

### Key findings

The controls over all of the they key financial system are sound.

Internal audit gave assurance for the following systems and included recommendations in their report as appropriate:

- Housing Rents Income
- Council Tax Income
- Business Rates Income
- Sundry Income
- Non-pay Expenditure

Where internal audit have already raised a recommendation relating to a particular system, we do not propose including the recommendation within our report.

KPMG had additionally tested the following areas:

- Cash
- Treasury Management

No control weaknesses were found.

We have not yet assessed the controls over grant income, benefit expenditure, capital expenditure and payroll expenditure. Many of the key 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.

System	Assessment
Financial reporting	3
Grant income	n/a
Housing rents income	3
Council tax income	3
Business rates income	3
Sundry income	3
Payroll Expenditure	n/a
Non-pay expenditure	3
Benefits expenditure	n/a
Cash	3
Treasury management	3
Capital expenditure	n/a

- Key:
- 1 Significant gaps in the control environment.
  - 2 Deficiencies in respect of individual controls.
  - 3 Generally sound control environment.

Internal audit complies with the *Code of Practice for Internal Audit in Local Government*.

#### Work completed

In order to maximise the efficiency of the audit function across the Authority, we work closely with Internal Audit to avoid duplication.

Where we intend to rely on internal audit's work in respect of the Authority's key financial systems, auditing standards require us to complete an overall assessment of the internal audit function and to evaluate and test aspects of their work.

*The Code of Practice for Internal Audit in Local Government* (the Code) defines the way in which the internal audit service should undertake its functions. We assessed internal audit against the eleven standards set out in the Code.

We reviewed internal audit's work on the key financial systems and re-performed a sample of tests completed by them.

#### Key findings

We have reviewed Internal Audit's work and are satisfied that they are compliant with the *Code of Practice for Internal Audit in Local Government*.

This is based on our reported assessment of Internal Audit in 2009/10, our assessment of their files and our knowledge from continual liaison with key personnel, review of documents and attendance at Audit Committee.

Based on our assessment, internal audit complies with the Code.

We did not identify any significant issues with internal audit's work and are pleased to report that we are again able to place full reliance on internal audit's work on the key financial systems.

Despite the changes of staff within the internal audit function, and the move to Riverside House, both of which could potentially have impacted on the quality of work produced we saw an improvement in

the clarity of internal audit's working papers compared to previous years.

Aspect	Assessment
Scope of internal audit	3
Independence	3
Ethics for internal auditors	3
Audit Committee	3
Relationships with management, other auditors and other review bodies	3
Staffing, training and development	3
Audit strategy and planning	3
Undertaking audit work	3
Audit strategy and planning	3
Due professional care	3
Reporting	3

Key:

- 1 Non-compliance with the standard.
- 2 Areas for improvement.
- 3 Full compliance with the standard.



There have been a number of updates to the Code of Practice for Local Authorities for the 2011 – 12 Year

Discussions are also taking place around the accounting treatment for RBT and Digital Region Ltd.

### Work completed

The Code of Practice for Local Authorities has been updated for the 2011/12 financial year. Key changes include:

- Adopting the requirements of FRS30, Heritage Assets;
- Amending the related party disclosures required and providing more guidance on the definition of a related party;
- Additional guidance on accounting for:
  - Pension strain;
  - Grants and contributions; and
  - the Carbon Reduction Commitment Scheme.

Discussions are also taking place around the treatment of RBT and Digital Region Ltd in the financial statements.

### Key findings

As part of our regular communications with the Strategic Director of Resources, Director of Financial Services and Finance Manager, we have discussed the above updates to the Code, RBT and Digital Region Ltd. The Authority has been very proactive in identifying where additional work is required to comply with the Code of Practice updates and bringing to our attention any areas which require discussion.

With regards to RBT and Digital Region Ltd, there are still on-going discussions as to the exact impact on the financial statements. However, again the Authority has been proactive at bringing these issues to our attention and providing clear working papers detailing their proposed accounting treatment.

## Key areas

The Authority has taken the key risk areas we identified seriously and made good progress in addressing them.

However, these still present significant challenges that require careful management and focus. We will revisit these areas during our final accounts audit.

### Work completed

In our External *Audit Plan 2011/12*, presented to you in February, we identified the key areas affecting the Authority's 2011/12 financial statements.

Our audit strategy and plan remain flexible as risks and issues change throughout the year. To date there have been no changes to the risks previously communicated to you.

We have been discussing these risks with the Strategic Director of Resources, Director of Financial Services and Finance Manager as part of our regular meetings. In addition, we sought to review relevant workings and evidence and agree the accounting treatment as part of


our interim work.

### Key findings

RMBC have taken these issues seriously and made good progress in addressing them. However, these still present significant challenges that require careful management and focus. We will revisit these areas during our final accounts audit.

The table below provides a summary of the work the Authority has completed to date to address these risks.

Key audit risk	Issue	Progress
	<p>As at November 2011, the Authority forecast an overspend on its Budget of £7.393m (3.4%). The main reasons for the projected overspend were the continued demand on services and cost pressures in looking after vulnerable children across the Borough; one off property costs relating to the continued rationalisation of the Council's asset portfolio to drive future efficiencies; and the extended timetable for realising the full forecast management and business support savings.</p> <p>The Authority currently estimates that another £20m in savings will need to be achieved during 2012/13 to address the further reductions to local authority funding. Against a backdrop of continued demand pressures in Children and Young People's Services it will become more and more difficult to deliver these savings in a way that secures longer term financial and operational sustainability.</p>	<p>The Authority is still facing cost pressures, however the revised forecast overspend for the year had reduced to £3.066m (1.4%) at the time of writing this report. Some of the initial costs have been mitigated through capitalisation of the Waste PFI, receiving additional NHS funding, and the proposed closure and use of some reserves.</p> <p>The Authority has also approved its budget for 2012/13, which included the required cost savings.</p> <p>The Authority continues to monitor its financial position and look at ways to reduce the forecast overspend.</p> <p>Prior to issuing our financial statements opinion, we will review the outturn for 2011/12 and review financial performance for 2012/13 against the budget.</p>

Key audit risk	Issue	Progress
	<p>The 2011/12 Code includes a number of accounting changes, including a new requirement to carry 'heritage assets' at valuation. Heritage assets include historical buildings, museum and gallery collections and works of art.</p> <p>The 2011/12 Code also clarifies requirements in a number of areas where ambiguity was identified in the 2010/11 Code.</p> <p>The Authority needs to review and appropriately address these changes in its 2011/12 financial statements.</p>	<p>There has been on-going discussions between the Authority and KPMG regarding the requirement in the 2011/12 Code in respect of heritage assets. The Authority has been able to justify its decision to not obtain valuations for the 2011/12 financial statements on the grounds the benefits of such an exercise are outweighed by the costs. The 2011/12 Code allows such a decision. We have also discussed the disclosure requirements for the 2011/12 financial statements. The Authority has also provided a plan for obtaining valuations for heritage assets for the 2012/13 financial statements that we are satisfied with.</p> <p>The Authority has considered other changes in the 2011/12 Code and we are pleased with the progress the Authority has made.</p>

**Our VFM conclusion considers how the Authority secures financial resilience and challenges how it secures economy, efficiency and effectiveness.**

**We follow a risk based approach to target audit effort on the areas of greatest audit risk.**

**Our External Audit Plan 2011/12 describes in more detail how the VFM audit approach operates.**

#### Background

Auditors are required to give their statutory VFM conclusion based on two criteria specified by the Audit Commission. These consider whether the Authority has proper arrangements in place for:

- securing financial resilience: looking at the Authority’s financial governance, financial planning and financial control processes; and
- challenging how it secures economy, efficiency and effectiveness: looking at how the Authority is prioritising resources and improving efficiency and productivity.

We follow a risk based approach to target audit effort on the areas of greatest audit risk. We consider the arrangements put in place by the Authority to mitigate these risks and plan our work accordingly.

Our VFM audit draws heavily on other audit work which is relevant to our VFM responsibilities and the results of last year’s VFM audit. We then assess if more detailed audit work is required in specific areas. The Audit Commission has developed a range of audit tools and review guides which we can draw upon where relevant.

#### Overview of the VFM audit approach

The key elements of the VFM audit approach are summarised below.



We have identified a number of specific VFM risks.

We will carry out additional risk-based work in the two areas.

#### Work completed

In line with the risk-based approach set out on the previous page, we have

- assessed the Authority's key business risks which are relevant to our VFM conclusion;
- identified the residual audit risks for our VFM conclusion, taking account of work undertaken in previous years or as part of our financial statements audit; and
- considered the results of relevant work by the Authority, the Audit Commission, other inspectorates and review agencies in relation to these risk areas; and
- concluded to what extent we need to carry out additional risk-based work.


#### Key findings

Below we set out our preliminary findings in respect of those areas where we have identified a residual audit risk for our VFM conclusion,

We will report our final conclusions in our *ISA 260 Report 2011/12*.

Key VFM risk	Risk description and link to VFM conclusion	Preliminary assessment
	<p>The Authority is seeking to end its partnership with BT and delivery of transactional services in RBT. There are significant initial costs and potential future savings and opportunities from such a change. Given the scale of costs and potential savings there is an impact on value for money.</p>	<p>The Authority undertook a value for money assessment in forming a decision to end its partnership with BT and delivering of transactional services in RBT. The Authority also identified a range of other considerations in forming its decision.</p> <p>We will now undertake a review of the value for money assessment that was undertaken including the considerations that took place. We will then be able to provide a view on the Authority's overall arrangements to secure economy, efficiency and effectiveness.</p>

## Specific VFM risks

Key VFM risk	Risk description and link to VFM conclusion	Preliminary assessment
	<p>The Authority's Joint Venture company, Digital Region Limited, has significant liabilities that the Authority (and other members of the joint venture arrangement) would need to fund if Digital Region Ltd ceased trading.</p>	<p>At the time of writing this report, the Authority was working with the other shareholders of Digital Region Ltd to form a decision on the future of the company. Our work will review the Authority's value for money arrangements in managing the potential issues concerning Digital Region Ltd.</p>

We have given each recommendation a risk rating and agreed what action management will need to take.

The Authority should closely monitor progress in addressing specific risks and implementing our recommendations.

We will formally follow up these recommendations next year.

Priority rating for recommendations		
<p><b>1</b> <b>Priority one:</b> 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.</p>	<p><b>2</b> <b>Priority two:</b> 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.</p>	<p><b>3</b> <b>Priority three:</b> 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.</p>

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
1	2	<p>We noted a number of instances where the process for removing user accounts assigned to leavers was not effective and there are areas for improvement as follows:</p> <ol style="list-style-type: none"> <li>Leavers on Cedar Financials – 8 user accounts assigned to leavers during the reporting period were still active at the time of our inspection. These accounts were subsequently removed as a result of our observation. Further inspection of these user accounts identified instances where 5 of the 8 accounts had been accessed after the user had left the Authority. We enquired of management and were informed that there are business reasons for accessing leaver accounts after their departure.</li> <li>Leavers on ICON Cash Receipting – 5 user accounts assigned to the leavers during the reporting period were still active at the time of our inspection. These accounts were subsequently removed as a result of our observation. Further inspection of these user accounts identified instances where 2 of the 5 accounts had been accessed after the user had left the Authority.</li> <li>Monitoring of ICON, PSe and Northgate users – We noted that no process is currently in place to review users of ICON for continued validity or appropriateness of access assigned. We also noted that the report used to monitor</li> </ol>	<p>Cedar - User accounts are subject to a quarterly security review. The 8 user accounts in question related to staff who left after the last review immediately prior to the period of audit had been completed. They would therefore have been picked up at the next review. Management consider quarterly review to be sufficient. Accounts such as the 5 user accounts referred to are sometimes enabled after the user has left the authority to allow failed processes to complete. The accounts are then re-disabled. In such circumstances, the system shows the 'last sign on date' as being the date the user account was re-disabled which may give the impression there has been a security risk. There is no risk from this process as all access rights are denied to prevent record creation or amendment. However, with immediate effect, a record will be kept of the reason for enabling a leaver's user account to provide an audit trail as recommended.</p> <p>ICON – The 5 user accounts referred to arose exceptionally because during the period that ICON was being upgraded between November 2011 and</p>



No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
1	2	<p>Northgate users is not sufficient enough in detail to allow the reviewer to monitor the appropriateness of access assigned. In addition, we noted that no evidence is retained of the monitoring conducted over users of PSe.</p> <p>These observations present a risk to the overall system security, which could lead to inappropriate access to key financial systems.</p> <p><i>Recommendation</i></p> <p>We recommend that the Authority reviews its approach to monitoring of user access and prioritizes this for the timely removal of leavers to key financial systems. In addition, where there is a business justification to access leaver accounts on Cedar Financials, an audit trail of such access should be retained.</p>	<p>go live on 2 February 2012 they were created in the test system and then transferred to the live system and were not therefore picked up by the normal process of disabling users based on information on leavers reports. Similarly, of the 2 user accounts referred to as having been accessed after the user had left, one was a test user whose last log in date of the 24 November 2011 pre-dated the go live date and therefore posed no risk. There is no record that the second user referred to ever having logged in to the system. Hence, in summary, management consider the current process of disabling users to be effective.</p> <p>PSe - The review process for PSe users is an automated job that immediately disables any accounts where an employee leaves or transfers organisational area. Our view is that the current process is sound on the reasonable premise that if an employee has not changed job (ie moved within an organisational area) then their access requirements will not have altered We do not believe that emailing Users/Managers every 6 months to confirm access requirements as has been suggested would enhance the process.</p> <p>Northgate - The Job Role associated with each user will be included in the next user review, scheduled for June 2012, to provide further detail as recommended.</p>

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
2	2	<p>We noted from inspection of the password parameters across key financial systems that a number were not in line with good practice standards as follows:</p> <ol style="list-style-type: none"> <li>1. ICON and Cedar password minimum length was set to 7 and 6 characters respectively</li> <li>2. The password history for PSe, Cedar and ICON was set to 3, 3 and 4 passwords respectively.</li> </ol> <p>These observations increase the risk to the overall system security.</p> <p><i>Recommendation</i></p> <p>We recommend that the password parameters for the ICON, Cedar and PSe systems are standardised where possible and in line with the Authority 's policies.</p>	<p>Agreed. Minimum password lengths and password history will be amended to bring them into line with ICT policy which requires a minimum password length of 8 characters and passwords to only be re-used after 20 changes. These changes will be implemented as follows:</p> <ul style="list-style-type: none"> <li>- Cedar - as part of the upgrade to 5.3 in May 2012.</li> <li>- ICON - already implemented.</li> <li>- PSe - password re-use in the process of being changed to 20.</li> </ul>

No.	Risk	Issue and recommendation	Management response/ responsible officer/ due date
3	2	<p>We noted from inspection of user accounts assigned privileges that a number were generic and in some cases not set to have expiring passwords as follows:</p> <ol style="list-style-type: none"> <li>1. A number of generic users on the Northgate system were noted. One such account is used for batch jobs but there are users with access to this account. In addition, there is a generic account used by the 3<sup>rd</sup> party supplier of the system for remote access for maintenance purposes.</li> <li>2. Users with access to the NO_UPDATE_PASSWORD profile are not required to change their passwords in line with password policies.</li> <li>3. An ADMIN user account was identified on the ICON system, which was used during the upgrade from Radius. We acknowledge that this account was removed at the time of our observation.</li> </ol> <p>The observations increase the risk of un-attributable user activity on key financial systems and where user accounts do not require password expiry, un-authorized and un-attributable user activity could be available for long periods.</p> <p><i>Recommendation</i></p> <p>We recommend that all user accounts, where possible, are attributable to users and those used for batch jobs are not accessible for day to day tasks by users. In addition, we recommend that all accounts where possible (i.e. acknowledging that some would result in jobs failing if password expiry is set) should have expiring passwords.</p>	<p>Northgate -There are only two generic users on the Northgate system. One is a Super User that is also needed for Unix access by the Unix Team for release upgrades. This is used for a very limited number of batch scheduler jobs due to the way that Northgate have set up permissions to a small number of batch scheduler modules. The 3<sup>rd</sup> party supplier generic user that is used for remote access system support is on a profile where a regular password is forced.</p> <p>Northgate - The number of users with the NO_PASSWORD_UPDATE profile has been reduced to 4. This privilege is needed to ensure that future batch scheduler jobs run successfully, as batch schedule jobs will only run if the password for the user is the same when the job is run that it was when the job was created. Batch scheduler jobs are created up to 6 months in advance.</p> <p>ICON – Overall security has been enhanced following the system upgrade by:</p> <ul style="list-style-type: none"> <li>- Changing the User Id Code from a 3 digit number to a person's name.</li> <li>- Introduction of a 90 day Password Expiry.</li> <li>- Adoption of a minimum password length of 8 characters and 20 password changes before a password can be re-used in accordance with ICT policy.</li> <li>- Passwords consisting of Alpha &amp; Numerical Characters.</li> <li>- A 180 minute Account Lockout Period &amp; a 90 day Inactivity Period.</li> </ul>

## Follow-up of prior year recommendations

The Authority has not implemented all of the recommendations in our Interim Audit Report 2010/11.

We re-iterate the importance of the outstanding recommendations and recommend that these are implemented as a matter of urgency.

This appendix summarises the progress made to implement the recommendations identified in our Interim Audit Report 2010/11 and re-iterates any recommendations still outstanding.

Number of recommendations that were:	
Included in original report	2
Implemented in year or superseded	2 partial
Remain outstanding (re-iterated below)	2 partial

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at 31 <sup>st</sup> March 2012
1	2	<p><b>IT Access Controls</b></p> <p>We identified a number of instances where user access controls were not operating effectively and / or there are performance improvement points that the Authority should consider.</p> <p>PSe Starters – some user request forms were not available to support new starters access to the system.</p> <p>Cedar Leavers – there were user accounts assigned to leavers that remained active.</p> <p>Radius Leavers – there were user accounts assigned to leavers that remained active.</p> <p>Cedar/PSe/Northgate Monitoring of users – evidence of review for these systems was not available.</p>	<p>The management for each service will review the ongoing effectiveness of the IT access controls and where appropriate consider the actions that need to be taken.</p> <p>September 2011</p>	<p>From inspection of controls during the 2011-12 reporting period, we noted the following:</p> <ul style="list-style-type: none"> <li>- the observation in relation to PSe Starters is now implemented</li> <li>- Cedar monitoring is now implemented</li> </ul> <p>However, the observations in relation to Cedar Leavers, Radius Leavers and PSe and Northgate monitoring remain outstanding and have been included in Appendix A.</p> <p>Although Cedar monitoring is now in place, we identified a number of leaver accounts that were removed following our observation during the 2011-12 reporting period.</p>

## Follow-up of prior year recommendations continued

No.	Risk	Issue and recommendation	Officer responsible and due date	Status as at 31 <sup>st</sup> March 2012
2	2	<p><b>IT General Controls – Password Security</b></p> <p>The password parameters for key IT systems were inspected and it was found that the password parameters for both Radius and Northgate were not as strong as they could be.</p>	<p>The management for each service will review the ongoing effectiveness of the IT access controls and where appropriate consider the actions that need to be taken.</p> <p>September 2011</p>	<p>This action has been implemented for Northgate but not for the upgrade of Radius to ICON and therefore has been included in Appendix A.</p>



*cutting through complexity™*

© 2012 KPMG LLP, a UK limited liability partnership, is a subsidiary of KPMG Europe LLP and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (KPMG International), a Swiss entity. All rights reserved.

The KPMG name, logo and 'cutting through complexity' are registered trademarks or trademarks of KPMG International Cooperative (KPMG International).