
**MANCHESTER CITY COUNCIL
REPORT FOR RESOLUTION**

REPORT TO: Audit Committee - 14 January 2010

SUBJECT: External Audit Recommendations
Quarterly Monitoring Report September 2009 to January 2010

REPORT OF: Assistant Chief Executive (Performance)

Purpose of Report

To provide a quarterly progress report on the implementation of outstanding recommendations from external audit work across the Authority by the Audit Commission and Grant Thornton during the last three audit years.

Recommendation

It is recommended that Committee note the report and advise on any further action the Committee wants to be taken.

Financial Consequences for the Capital and Revenue Budgets

None identified.

Contact Officers

Sharon Kemp	0161 234 3910	sharon.kemp@manchester.gov.uk
Andrew Blore	0161 234 1882	a.blore@manchester.gov.uk

Background Documents

Audit Reports listed under Para 2.1.

Wards Affected

N/A

Implications for Key Council Policies

Anti-Poverty	Equal Opportunities	Environment	Employment
None	None	None	None

1 **Introduction**

1.1 The implementation of recommendations included within external audit reports issued during the last three audit years are routinely monitored on a quarterly basis by the Corporate Performance Group. This report provides progress against audit recommendations for the last quarter (October to December 2009).

2 **Process**

2.1 A meeting was held with Grant Thornton to identify all the outstanding external audit reports. As a result of this meeting four new external audit reports were identified. These reports are listed below:

- Grant Claims and Returns
- Annual Report to those Charged with Governance
- Information Systems Controls
- SAP Follow up report

2.2 The leads for each of the external audit recommendations were then asked to complete a proforma that would detail the progress made around that specific recommendation. This information was then collated into this report.

2.3 The outstanding external audit report has been changed this quarter to include more detailed information on the action being taken to complete recommendations and the timescales for when the actions and the recommendation will be completed.

3 **Progress against Outstanding Recommendations**

3.1 A summary of reports with outstanding recommendations is provided in Appendix 1.

3.2 Appendix two contains progress against each of the outstanding recommendations and the date the recommendation will be completed. Progress has been made against a number of these recommendations since the last monitoring report and where recommendations are outstanding or have not been fully implemented, further details are given below.

SUMMARY OF AUDIT REPORTS WITH OUTSTANDING RECOMMENDATIONS

Audit Report	Issued	Recommendations Implemented as at September 2009	Recommendations Implemented as at January 2010	Management Assurance Statement
Improving Outcomes through Joint Working	November 2007	9/12	11/12	Risk of late implementation is minimal as appropriate arrangements have been made for service delivery.
Review of Internal Audit	January 2008	8/11	8/11	As the Head of Internal Audit and Risk Management consider this to be a low risk as staff use a suite of standard documents and supported through management review.
Review of Internal Audit	June 2008	12/13	12/13	As a result of the compensating controls (all staff are fully or part qualified to professional standards, all files are confirmed as reviewed by a Lead Auditor / Manager, senior management spot reviews of files) the Head of Internal Audit and Risk Management considers this to be low risk.
Data Quality	November 2008	0/2	0/2	Risk is minimal as identified actions are being implemented and are on track to be completed within identified timescales.
Governance	March 2008	0/1	0/1	Risk is minimal as work is ongoing and identified actions are being implemented and progressed.
Review of the Management of External Funding	June 2008	8/10	9/10	Risk is minimal as identified actions are being implemented and progressed.
Review of Risk Management	July 2007	10/16	12/16	The risk to achievement of these is largely centred on resources and the appointment of staff to support management in the embedding of risk and support in the delivery of training. These recommendations are to be considered as a medium risk as our ability to drive this agenda forward is dependent on the rest of the Council and our ability to provide

				corporate support.
Grant Claims and Returns 2007-08	January 2009	-	11/14	Risk is minimal as identified actions are being implemented and are on track to be within identified times scales.
Annual Report to those Charged with Governance	September 2009	-	1/6	The risk is small as arrangements have been put in place to address these issues.
Information Systems Controls	November 2009	-	1/14	Risk is minimal as identified actions are being implemented and progressed. ICT are working with Ernst and Young as strategic partners to assist with the development of strategic plans and operational IT policies.
SAP Follow Up Report 2008/09	July 2009	-	1/4	Whilst there are no longer any SAP-specific security posts within the ICT Service, risks have been mitigated through the establishment of the SAP Security Working Group (see Recommendation R2) which has a remit to oversee all SAP security-related issues and to ensure that any necessary actions are undertaken to affirm the judicious management of SAP from a security perspective.

PROGRESS AGAINST OUTSTANDING AUDIT RECOMMENDATIONS

Report: Improving Outcomes through Joint Working, November 2007

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>R9 Explore the potential benefits for arrangements to share asset financial information between the PCT and Council.</p>	<p>Lydia Morrison</p>	<p>Date not yet known</p>	<p>The PCT are currently undergoing extreme budgetary pressures, which means that they have stopped engaging in the work to complete this action.</p> <p>Colleagues in the PCT are being continually chased and it is hoped that a meeting with the PCT head of estates will be held later this month. The treasurer is aware of the lack of progress against this recommendation.</p>
<p>R10 In relation to the relocation of C&YP services multi-agency teams:</p> <ul style="list-style-type: none"> • identify the financial impact of vacated premises once staff are relocated to new locations; and • ensure matched funding for 2008/09 is agreed from both the Council and the PCT to maintain project delivery. 	<p>Allan Seaborn (Children's Services)</p>	<p>N/A</p>	<p>This recommendation and R11 related to plans prior to 2007 to establish fully integrated multi-agency Children and Young People Teams which would have been managed by a single manager from one of the constituent agencies, as part of the developing Children's Trust arrangements.</p> <p>It became clear by 2007 that this model was not deliverable at that time in Manchester. A decision was taken to follow a model, which aligned resources in delivery with those of the NHS and other partners, rather than pursuing fully integrated teams.</p> <p>Work has progressed effectively through this model, which has been supported by tools such as the Common Assessment Framework. Children's Trust arrangements are being further developed but to date the recommendations in 10 and 11 have not been needed, as the teams/project did not continue in the same form.</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
R11 Put in place measurable benefits, targets, a current baseline position and performance management arrangements for the physical activity and C&YP multi-agency teams' joint use of assets, to ensure the projects' outcomes and successes can be effectively assessed.	Colin Cox, Ann Inman (physical activity) Allan Seaborn (Children's Services)	N/A	Please see the information in R10 on page 5.

Report: Review of Internal Audit, January 2008

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
R9 The internal audit quality manual, when produced, should include procedures to: standardise the electronic and paper file structure; ensure that each file contains systems documentation and description of walkthrough testing; incorporate CIPFA key control into job planning.	Tom Powell Internal Audit	April 2010	<p>Considered a low risk issue by Head of Service as the key elements of the audit approach are in place but have not been consolidated into a manual. For example, file structures are relatively standard and all documentation / testing is completed in standard documents. Auditors use standard planning documents, monitoring and reporting templates and these include the requirement for walkthrough testing on all system and compliance audits. CIPFA key controls are used as reference for all audits, especially relevant for work on the core financial systems where they form the basis for testing programmes.</p> <p>In terms of progress, the basic structure for the audit manual has been determined. Initial plans to produce an audit manual have been superseded by a decision to upgrade the electronic</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
			<p>working papers system to reflect changes to the audit approach (new reports, approach to monitoring recommendations etc) that is proposed for the new audit plan year starting in April 2010. The audit manual completion will coincide with this development as well as the return to work of a manager who returned from sick leave in December.</p> <p>This also allows for all members of the audit team to be involved in the development of the manual and this approach will help ensure its contents are embedded at the outset and be far more than simply a source of reference.</p>
<p>R10 To be fully compliant with the code a monitoring and review programme to ensure that due professional care is achieved and maintained should be developed.</p>	<p>Tom Powell Head of Internal Audit</p>	<p>April 2010</p>	<p>Considered a low risk issue by Head of Service as a number of compensating controls exist:</p> <ul style="list-style-type: none"> • the role of Lead Auditors and Audit Management provides quality review and quality assurance • electronic files cannot be closed without supervisory review and sign-off of all audit work • Audit management attend planning and completion meetings for all audits and assignments to ensure that the work is planned appropriately and that work supports audit opinions. <p>These arrangements will be codified in the Audit Manual due for completion by April 2010.</p>
<p>R11 The quality assurance process framework, building on the items set out in paragraph 41 should be finalised.</p>	<p>Tom Powell Head of Internal Audit</p>	<p>April 2010</p>	<p>This is the same issues as referred to in R10 so is considered to be low risk.</p>

Report: Review of Internal Audit, June 2008

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
R9 The internal audit quality manual, when produced, should include procedures to: standardise the electronic and paper file structure; ensure that each file contains systems documentation and description of walkthrough testing; incorporate CIPFA key control into job planning.	Tome Powell Head of Internal Audit	April 2010	As per response to R9 on the previous page.

Report: Data Quality, November 2008

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
R1 The Council should review systems used to capture performance information to ensure that data input is "right first time" and does not require significant manual adjustments to produce reliable and accurate	Jane Abdulla/ Andrew Blore	July 2010	Work is being progressed with internal audit to assess systems and process used within services to ensure data is input 'right first time'. The first stage of this assessment is conducted using the data quality checklist questions, which on completion are used to risk assess each performance indicator. This risk assessment includes an analysis of the amount of manual manipulations of data. The second stage of the process is a series of data quality

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
information.			audits. The data quality audits will be conducted on every Local Area Agreement indicator and the National Indicator Set. Each performance indicator will be assessed on reliability, accuracy, validity, timeliness, relevance and completeness. Any problems identified will be tackled through targeted action plans. The data quality audits for the high-risk performance indicators data quality audits began in November 2009. The data quality audits for the low and medium risk indicators will begin in February 2010 and continue throughout 2010. The data quality audits are also targeted towards Partner organisations. Manchester Fire, the PCT, GMPTE and GMP are all engaged in the data quality audit process.
R2 The Council should implement arrangements to ensure compliance with Data Quality principles and procedures through regular Training and support for staff and managers involved in the preparation of key performance information.	Jane Abdulla/ Andrew Blore	March 2010	<p>Two training sessions on data quality have already been facilitated. A series of 45-minute training sessions tailored to the specific needs of officers and managers will be delivered on the 1 February 2010 and 1 March 2010 respectively. The Partnerships and Performance Team and Grant Thornton will jointly facilitate these training sessions. The MCC data security officer has also agreed to attend the training sessions and talk about the importance of data sharing and data security. The data quality training sessions are targeted not only toward MCC staff but also to officers and managers in Partner organisations. Manchester Fire, the PCT, GMPTE and GMP have all agreed to send officers to the data quality training sessions.</p> <p>The data quality pages on the intranet are regularly updated to provide on-line support on data quality for officers. An on-line quiz designed to help officers identify data quality issues can be found on the intranet pages.</p>

Report: Governance, March 2008

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>R2 Challenging assurances and resolving previous issues: The Council should ensure that previously identified areas of weakness within partnership management arrangements and in the Council's recent partnership arrangements self assessment, are used to review and challenge partnership assurances and to feed into management arrangements improvement plans. In particular, the Council should focus attention on a number of areas that will form part of the use of resources assessment: demonstrating the value for money of partnership working;</p>	<p>Jane Abdulla/Emma Burnett</p>	<p>April 2010</p>	<p>In order to take the Partnership Governance Framework (PGF) forward work is being undertaken to further improve arrangements for services to provide assurance on an ongoing basis that appropriate partnership governance is in place and is operating effectively. In particular, two workstreams are currently being taken forward as follows, and will be completed by April 2010: -</p> <ol style="list-style-type: none"> 1. Partnership classification. A revised approach to partnership registration and self assessment is currently being developed, with the objective of linking the assurance framework to the risk profile of the individual significant partnerships. This will thereby focus resources upon obtaining a greater degree of assurance from and providing additional support to those partnerships which are classified as being the highest risk. 2. Identification of all partnerships. Work is also continuing to develop a register of all of the Council's partnerships (in the widest definition), all of which should be operating within the parameters of the PGF, in order to inform ongoing partnership assurance and risk assessment activity.

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>consistently approving business cases before entering into partnerships, including the costs to the Council against the expected benefits; joint strategic needs assessments, including an understanding of inequalities, that drives forward long term commissioning decisions and partnership objectives; improving evidence of joint service and financial planning through the Medium Term Financial Plan and service business plans; expanding joint procurement, asset management, IT and data quality arrangements; obtaining assurance over significant partners' business continuity plans.</p>			
<p>R2 continued - Evidencing partners' confidence in the arrangements for partnerships, inc. standards of conduct and governance arrangements; introducing robust risk management arrangements for partnerships; embedding robust performance</p>	<p>Jane Abdulla/ Emma Burnett</p>		<p>Please see information in R2 on page 10 of the report.</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>management arrangements for all significant partnerships, based on corporate standards for performance management, and including benchmarking of outcomes and indicators against others; implementing a procedure for declaring conflicts of interest within partnership organisations; considering whether there is a requirement for scrutiny to review any other significant partnerships (based on the outcome of the evaluation exercise); ensuring that the internal audit plan responds to key risks identified by the evaluation process; linking the PGF to the wider assurance framework; widening systematic feedback on how services are performing and demonstrating how this assists in making improvements to services; introducing systematic joint processes for managing the environmental impact of delivery of public services in Manchester.</p>			

Report: Review of the Management of External Funding, June 2008

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
R7. The Council should ensure the blue file methodology is consistently applied across all services, and appropriate training is provided to officers for all significant externally funded projects where there is no documentation standard prescribed by the funding organisation.	Carol Culley Head of Financial Management	Partially complete fully complete April 2010	The best practice from the blue file methodology has been incorporated into the grants protocol. The blue file methodology is fully embedded for European funding. It now needs to be promoted and rolled out for other areas of significant funding where defined specific grant methodologies by the funding body are not in place.

R9. To ensure awareness of co-ordinated grant claim arrangements across services, the grant claim co-ordinator should re-issue guidance to all services and deliver training where required.	Carol Culley Head of Financial Management	Complete	The revised Grants Protocol was issued on 30 September, following a review by Internal Audit.
--	--	----------	---

Report: Review of Risk Management July 2007

Recommendation	Responsible Officer	Recommendation Completion date	Assurance Provided By Service <u>(Including Risks)</u>
R5 The Council should address with partners how partnership risk management will work in practice, as part of implementation of actions to clarify and strengthen its own processes.	Tom Powell, John Gill	April 2010	<p>Assessed by Head of Service to be medium risk as successful delivery is dependent on engagement of partners in this process. Whilst risk management has developed during 2009 and further work is planned for early 2010 we need to continue the focus on partnership risk management to ensure this is embedding and working in practice.</p> <p>Areas of positive assurance include:</p> <ul style="list-style-type: none"> • Partnership risk management strategy and strategic risk register

			<p>in place- due to be refreshed in January 2010. All Thematic Partnerships have engaged in scrutiny of the strategic risks and in generating their own risk analysis in relation to their potential impact on their work programmes.</p> <ul style="list-style-type: none"> • Tailored risk management training to be provided to Partnership Management Group and Thematic Partnership Committees between January- March 2010. Approach endorsed by Management Group in November 2009. Sign off awaited from PSB. • Corporate Risk Management Team also involved with significant partnerships in undertaking strategic risk assessments, e.g. Housing Loop, Greater Manchester Resilience Forum, Crime and Disorder and Public Realm Risk.
<p>R6 The Council should ensure that departmental risk registers are further developed to more consistently describe risks, consequences and mitigating controls.</p>	<p>Tom Powell, John Gill</p>	<p>Partially Complete. Fully Complete June 2010</p>	<p>Assessed as low risk as registers improved significantly in 2010-13 business plans. There are some elements of inconsistency of detail and description in business plans but this represents good progress from previous years.</p> <p>2010/13 business plans included risk registers for each service. The challenge set out in this recommendation as well as R7 and R8 below is to develop how well judgements are explained, assurance over risks is obtained etc as well as demonstrating the ongoing management of risks.</p> <p>Assurance over work to date and the delivery of further improvement includes:</p> <ul style="list-style-type: none"> • Training being provided to all officers at Grade 7 and above as a rolling programme. 400 officers currently trained with additional target areas identified to receive training during the remainder of the financial year. Training specifically covers risk description, consequence analysis and approach to the identification and delivery of mitigating controls. • Guidance including in business planning guidance for 2010-13.

			<ul style="list-style-type: none"> • Good progress in describing risks reflected in 2010-13 business plans. • The Council has recruited two corporate risk managers, with a third post still to be filled (see R15 below). A primary role for the post holders, in addition to providing training and facilitated workshops for operational services, is to provide direct support to Heads of Service and Divisional Management Teams in developing risk assessments and delivering against programmes of mitigating control. • An assessment of how risk registers are being embedded will form part of the responsibilities of corporate risk managers and will be completed to provided evidence of embedding between April and June 2010.
<p>R7 The Council should ensure that departmental risk registers: clearly show how mitigating controls will manage the risk, explain the basis of the judgement on acceptability of residual risk and set out how assurance will be obtained over the effectiveness of operation of mitigating controls; allocate management of the risk to a named individual and set a deadline for implementation of any actions on mitigating controls.</p>	<p>Tom Powell, John Gill</p>	<p>Partially complete Completion by June 2010</p>	<p>As with R6 this recommendation relates to the quality of departmental risk registers. As above it is assessed as low risk as registers improved significantly in 2010-13 business plans. There are some elements of inconsistency of detail and description in business plans but this represents good progress from previous years and plans / resources in place should support further improvement during 2010.</p>

R8 The Council should ensure that departmental risk registers are updated throughout the year to evidence ongoing management of risks.	Tom Powell, John Gill	Partially complete Completion by June 2010	As with R6 this recommendation relates to the quality of the use of departmental risk registers. As above it is assessed as low risk as registers improved significantly in 2010-13 business plans. There are some elements of inconsistency of detail and description in business plans but this represents good progress from previous years and plans / resources in place should support further improvement during 2010.
R9 The Council should evidence that it has considered the risk of fraud and corruption when compiling and updating risk registers.	Tom Powell, John Gill	Complete	Risk mitigated as action completed Fraud and corruption is one theme that service management teams are encouraged to consider when compiling risk registers. Also an area considered when assessing financial and reputational risks in the identification of departmental and corporate risks. It is specifically referred to within risk management training and services that identify it as an issue of particular significance include it within their risk registers. A central assessment of fraud and corruption risks is provided by the Internal Audit Anti Fraud and Investigation Team and the Fraud Investigation Group.
R15 The Council should improve staff resource to support Strategic Management Team and departmental management in managing risk.	Richard Paver	Complete	Risk mitigated as action completed 3 additional Risk Manager posts advertised in November 2009. Interviews took place on 17 December 2009. Two candidates appointed. Plans to secure resources to fill the additional third post to be determined during December 2009.

Report: Grant Claims and Returns 2007/08

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
----------------	---------------------	--------------------------------	---

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>R1 The Council should review its procedures for the certification of grant claims and returns and appoint a central grants coordinator responsible for identifying and monitoring all claims against submission deadlines.</p>	<p>Steve Carey</p>	<p>Complete Ongoing (TBC)</p>	<p>The revised grants protocol was issued 30/09/2009. A grants co-ordinator role has been established within the Strategic Planning Team, this role is responsible for monitoring the completion of grant claims against submission dates. The position is currently vacant and is being partly covered by another member of the team. It will move back to the Revenue Finance Team as soon as the resources are in place to take it over. Interim resources have been secured to cover this activity.</p>
<p>R2 The Council should review and update the grants protocol and issue this to all officers responsible for the compilation of claims and returns.</p>	<p>Steve Carey</p>	<p>Complete</p>	<p>The revised grants protocol was issued 30/09/2009 to heads of Finance who circulated it to relevant heads of service and other finance and non-finance staff dealing with grants.</p>
<p>R3 In order to avoid possible sanctions and penalties from the grant awarding body, the Council should submit claims and returns to external audit by the prescribed audit deadline. Grant preparers should allow sufficient time for review, sign off and posting of claims.</p>	<p>Steve Carey</p>	<p>Complete</p>	<p>This requirement is included in the revised grants protocol. Sufficient time must be allowed for verification checks to be carried out by the reviewing officer and for the Treasurers signature to be obtained – it is suggested two weeks is allowed for this process. The Grant Co-ordinator will monitor that grants are being processed in line with agreed deadlines. One month before the submission is due to external audit a reminder is sent to the nominated contact officer for the grant – confirming the deadline. Grant claimants must inform the grant co-ordinator of any claims which may not meet the agreed deadline, the grant co-ordinator will keep External Audit informed and escalate within the department if necessary.</p>
<p>R4 In order to reduce the level of amended and qualified claims, grant claim preparers should ensure they consult the relevant</p>	<p>Steve Carey</p>	<p>Complete</p>	<p>A certification checklist is included as Appendix A to the revised Grants protocol. This asks the officer to confirm the claim has been completed in accordance with the specified instructions.</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
they consult the relevant guidance notes when compiling claim forms. This should be evidenced on a 'certification checklist'.			
R5 The Council should remind claim preparers that Certification Instructions are available for all grants from the grants co-ordinator. Preparers should review both awarding body terms and conditions and Certification Instructions before compiling the claim form and supporting evidence files.	Steve Carey	Complete	The grants co-ordinator will receive the Certification Instructions from external audit as soon as they are available and will pass these on to the relevant officer. As above a certification checklist is included as Appendix A to the revised Grants protocol. This asks the officer to confirm the claim has been completed in accordance with the specified instructions. They are also informed that working papers must provide a complete audit trail and must comply with the Certification Instructions.
R6 All claims submitted to external audit should be subject to an independent review either by the line manager of the claim preparer or the grants co-ordinator.	Steve Carey	Complete	As per the revised grants protocol all claims submitted to external audit have a named grant claimant officer and a reviewing officer who will 'sense check' the claims form and ensure the supporting working papers provide a strong audit trail. This officer should be a senior manager of the grant claimant or a finance officer.
R7 Departments should identify an appropriate responsible officer for each claim and return and inform the grants co-ordinator of any changes.	Steve Carey	Complete	The grant register identifies the claims preparer and reviewing officer for each claim which is subject to external audit, if this changes the grant co-ordinator must be informed as soon as possible.

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>R12 The Housing department should improve the audit trail for eligible administrative expenses for the pooling housing capital receipts return.</p>	<p>Paul Hindle</p>	<p>31st March 2010</p>	<p>No administrative expenses have been charged to capital receipts return until eligibility has been determined, once happy with eligibility they will be included in the quarter 3 return.</p> <p>Charging departments have been made aware, that we can only claim costs in respect of completed sales. Costs in respect of aborted sales will need to be charged to revenue, and this will create additional budget pressures.</p> <p>Charging departments have also been made aware of the need to revisit the basis of recharges, as the costs have been charged on an historic apportionment basis, but given the significant reduction in the numbers of right to buys completed, this is not appropriate anymore.</p> <p>The administrative charges included within the current years return, will be supported by a working paper setting out the charges and which properties they relate too.</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
R1 The Council should ensure receipts in advance are correctly recorded within the financial ledger, ensuring departments are clear of the accounting requirements	Karen Gilfoy	March 2010	<p>Guidance will be issued to departmental finance staff on the accounting treatment of receipts in advance as part of the Council's year-end closedown procedures. This will also be discussed with the departmental closedown coordinators at the meetings held during the closedown of the Council's accounts. The guidance will include details of the correct coding of receipts in advance and when income received should be treated as receipts in advance.</p> <p>The 2009-10 closedown timetable will include a task to be completed by a member of the Financial Accountancy team to check the coding and supporting evidence of all receipts in advance over £250k.</p>
R2 As part of year end bank reconciliation, the Council should review cheques raised at the end of the year and restate any cheques not issued.	Karen Gilfoy	31 March 2010	A process will be put in place by Financial Accountancy, with the Finance Shared Service Centre, to identify all cheques raised but not issued by 31 March 2010. These cheques will be classed as creditors rather than cash in the 2009-10 accounts.
R3 The Council should ensure all assets are valued on the correct basis in accordance with the SoRP guidance for updating valuations following reclassifications.	Karen Gilfoy/Mike Robertson	March 2010	Upon reclassification of an asset by Financial Accountancy and Corporate Property staff instructions are issued to the contracted valuer to revalue the asset in accordance with the SORP guidance. These valuations will be provided in March 2010.

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>R4 The Council should ensure supporting documentation is maintained to support assumptions used in all desktop revaluations.</p>	<p>Mike Robertson</p>	<p>Completed December 2009</p>	<p>The Housing Stock desktop revaluation has been completed in accordance with Government and RICS guidelines. Supporting documentation has been retained on file. Referencing of evidence has been included on the valuation against each Beacon and variant properties.</p> <p>My comments highlight the potential problems encountered using this method of valuation, but as it is proscribed by Central Govt and the RICS there are no methodological ways of mitigating the risk. A full revaluation is undertaken externally every five years, but this is still prone to the same risks as these relate to the application of 'beacon' values across a varied stock.</p>
<p>R5 The Council should review coding within the SAP ledger with a view to minimising the amount of manual adjustments required, and increase efficiency in producing the accounts.</p>	<p>Karen Gilfoy</p>	<p>January 2010</p>	<p>A meeting with Business Support was held in November to look at SAP reports available and how these can be used to reduce the number of manual adjustments required to produce the accounts.</p> <p>A report has been identified in SAP that can be adapted so that a number of the manual adjustments required to produce the accounts are done by SAP. A change request to adapt this report will be submitted.</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
R6 The Council should review the repairs and maintenance debtors on the housing rents system and remove erroneous debtors and associated bad debts.	Mark Slater	March 2010	<p>The rechargeable repairs accounts which were set up in error have now been fully reviewed and the reason(s) for the error(s) have now been identified. The majority of the errors occurred shortly after the introduction of a new computerised Housing Management System and came about as a result of a one off debit charge being set to be applied over a number of weeks / periods.</p> <p>The teams responsible for applying these charges have been made aware of the errors and have amended their set up procedures.</p> <p>The accounts set up incorrectly are being reviewed case by case and the appropriate adjustments being applied .</p>

Report: Information Systems Controls

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
1.We recommend that ICT Management ensure target deadlines to complete process documentation are met so that controls are consistently applied across the ICT department. This is important particularly with new ICT support staff joining the Council. Process documentation is critical but even more so in a changing	Steve Park	April 2010	<p>Although a manual process, Citrix server patches are kept up to date. Focus in the last four months has been on patching non-citrix servers to remediated critical vulnerabilities. Citrix server management will be incorporated into the broader Server Patch Management Process.</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>environment such as that being experienced by the Council.</p> <p>There is a monthly management report provided to give high-level feedback on the Microsoft server patches implemented and any outstanding risks. However, this does not include the Citrix servers. No formal management reporting is in place for Citrix server patches.</p>			
<p>2. We recommend a similar process for management reporting, i.e. email distribution and monthly reporting, be implemented for Citrix server patches. Senior ICT Management team members will therefore be aware of the patches that will be applied to the Citrix servers, and will receive assurance that patches are evaluated/approved and tested before deployment.</p>	Steve Park	April 2010	Management action, as above for recommendation one.

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>3. We recommend that the IT Security Policy is updated as soon as the partnership with Ernst and Young comes into effect.</p>	<p>Steve Park</p>	<p>April 2010</p>	<p>The Corporate ICT Security Policy will be re-written in light of lessons learned in 2009, latest best practice and planned deployment of new technology in 2010. This will be a priority action, along with the Corporate ICT Desktop Policy, with Ernst and Young.</p>
<p>4. We recommend that Management evaluate the need for multiple domain administrator accounts. While we expect administrators to have up to two accounts, we expect one of the accounts to be given lower privileges as this would be for day-to-day use.</p>	<p>Steve Park</p>	<p>January 2010</p>	<p>It is expected that this will be addressed by reducing the number accounts available to staff.</p>
<p>5. We recommend that IT management complete the IT centralisation project and develop centralised IT policies, to cover:</p> <ul style="list-style-type: none"> • Setup/modification and removal of user access for the network and applications; • Program change requirements for the application systems development process • that includes quality assurance, testing, and 	<p>Steve Park</p>	<p>Work Ongoing Priority plan complete December 18 2009</p>	<p>Management has engaged Ernst and Young as a strategic partner for the ICT Service to assist in the development of strategic ICT plans and operational IT policies. A preliminary plan of action based on strategic initiatives with timelines is expected to be completed by mid-December 2009.</p> <p>Ernst & Young have been engaged as Strategic Partners and a priority plan for 2010 that refers to the policies \ actions listed in the recommendation is being drafted, this will be complete by Dec 18.</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>migration to the 'live' environment;</p> <ul style="list-style-type: none"> • Software development, acquisition and implementation policy; • Virus management policy; • Firewall policy; • Data Security policy; • Domain policy (including audit policy, password policy and account lockout policy); • System backups and recovery policy; • Disaster Recovery and Business Continuity policy; and • Physical Security policy. <p>Once developed, the policies should be approved by senior management and applied across the Council.</p>			

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>6. We recommend that lists of access levels that require individual authorisation be identified. The list should be issued to the Service Support team for reference. This will help ensure that any separately requested access to systems is not copied over from the template account and that approval is properly obtained for the system as required.</p>	<p>Steve Park</p>	<p>March 2010</p>	<p>A start \ leaver \ user access amend process will be developed that will include the deletion of inactive accounts. ICT management note the risk posed by this issue, however to date resource has been prioritised on more serious threats.</p>
<p>7. We reiterate our original recommendation to implement a formal and regular process to review users and access. This should be done as a matter of priority.</p>	<p>Steve Park</p>	<p>June 2010</p>	<p>To address the complex process of account transfer this is linked to several other processes and will be addressed following starters and leavers.</p>
<p>8. We recommend that the monthly management report includes the reporting of risk of servers not detected and potentially not patched by WSUS.</p>	<p>Steve Park</p>	<p>January 2010</p>	<p>This will be included in monthly management reports, facilitated eventually by the network monitoring solution</p>
<p>9. We recommend Management take measures to reassess the vacant roles and the ICT security</p>	<p>Steve Park</p>	<p>January 2010</p>	<p>The staff consolidation is expected to be completed by end of January 2010. The revised ICT restructure provides distinction between IT security management and IT operations.</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>requirements of the Council as soon as possible, in order to ensure that all of the required IT security roles are undertaken and achieve a clearer distinction between IT security management and IT operations.</p>			<p>The ICT Service has been restructured to remove siloed functions, inherent single points of failure, and to provide adequate levels of support, i.e. in and out of hours.</p> <p>Management and leadership capabilities have been improved through the recent appointments of a Chief Information Officer, Head of ICT Operations and a Head of ICT Strategy and Change. IT operations and IT Security fall under the command of the Head of ICT Operations, led by different Operations Managers. The Head of Strategy and Change is focused on developing and prioritising the ICT Service roadmap and developing relationships with customers in service areas across the Council.</p>
<p>10. We recommend the following to be considered during further development of the DR Plan:</p> <ul style="list-style-type: none"> • Define a minimum acceptable recovery configuration for key businesses and systems; and • Outline a testing strategy <p>An alternative site has been identified to host the data centre away from the city centre. This site has been obtained in conjunction with the Manchester Digital Development Agency (MDDA) and offers improved</p>	<p>Steve Park</p>	<p>April 2010</p>	<p>The points are noted and will be incorporated into the next development of the ICT DR Plan that will be undertaken in conjunction with Ernst and Young.</p> <p>The DR Plan is an initial plan only and will developed further and tested throughout 2010. The initial plan contains:</p> <ul style="list-style-type: none"> - all emergency contact numbers, individuals and their roles, and their access methods, - all emergency contact numbers for site mangers, ICT support partners and utility suppliers, - details of where the plan is stored and accessed by staff, - high level risk assessment with probability scoring and consequence narrative, - DR plan trigger events and Emergency Management Team responsibilities, - Disaster Recovery Team and their responsibilities, - procedures to follow on discovery of an emergency, - media strategy - insurance details

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>(MDDA) and offers improved environmental conditions, security and recovery capabilities. The new data centre is a key part of the Council's ICT disaster recovery planning. It is expected that the data centre will be fully operational by March 2010. We understand that the Town Hall refurbishment will commence after the relocation of IT facilities to the new centre.</p>			<p>- financial impact assessment process</p>
<p>11. We recommend that IT complete the revision and agreement of the Information Security Policy and also develops an IT Acceptable Use Policy. The new policy should provide users with an understanding of the policy, its purpose, guidelines for following security practices, and definitions of their responsibilities.</p> <p>All users should be required to acknowledge their acceptance of the new policy and renew acceptance with any revision of the policy. Due to the number of users</p>	<p>Steve Park</p>	<p>January 2010</p>	<p>The Acceptable Email Usage policy has a revised date for completion - end January 2010 - due to other issues being given priority.</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
we would consider it practical to obtain and record user's acceptance of the policy as part of their login to the network.			
12. We recommend the screensaver password be enabled within the domain security settings to enforce users to log in again after 15 minutes of inactivity.	Steve Park	January 2010	Screensaver passwords will be activated to force a re-login after 15 minutes.
<p>13. System and security event logs should be reviewed and evaluated on a regular basis. The procedure should be formalised and the outcome of reviews should be documented.</p> <p>We recommend that ICT Management set this to "Success, Failure" to help determine any unauthorised changes which could indicate mistakes by an administrator or deliberate attacks.</p>	Steve Park	Complete December 2009	<p>Currently log 'success' but not 'failures'. These will start to be logged.</p> <p>This recommendation will be complete by the end of December</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provided By Service (Including Risks)
<p>14. We recommend a review of the life cycle for software licences, including their purchase, installation, reallocation and reconciliation. Although it is acceptable for different members of staff to be responsible for different licences, IT needs to clearly establish which staff are responsible for each stage of the life cycle.</p> <p>This should be centrally documented and managed by a small number of staff. Management may also consider taking measures to restrict users to being able to install their own software. This may also coincide with the removal of local administrators (see also recommendation</p>	<p>Steve Park</p>	<p>June 2010</p>	<p>A Configuration and Licensing Manager's post has been created within the new structures. It is hoped this post will be filled by January 2010. The Council will utilise the proposed monitoring system to manage its software licensing arrangements.</p> <p>Completion date will be June 2010.</p>

Report: SAP Follow Up Report 2008/09

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provide By Service (Including Risks)
<p>R1 We recommend that for out of hours access procedures are developed where a user can be unlocked for a period of time, and subsequently locked after the work has been performed.</p> <p>If out of hours access is occurring on a regular basis and therefore this is unfeasible, we would also recommend that the Council reviews the reasons for this maintenance and whether it is indicative of underlying issues that need to be resolved.</p>	<p>Phil Burke</p>	<p>February 2010</p>	<p>At the present time some support staff have unconstrained access to transactions which are deemed 'sensitive' within the SAP system. The issue is being addressed through a comprehensive review and re-design of all SAP roles assigned to support staff, and re-design work is in progress with the intention of implementing the new roles at the earliest possible opportunity. In parallel with the above work, a program has also been developed to assist with the regular monitoring of users having access to sensitive transactions.</p> <p>In relation to the assignment of standard SAP profiles (which provide wide-ranging SAP access) this is now limited to members of the SAP Basis team who occasionally require extensive access for emergency intervention work outside normal office hours. This type of support is the exception rather than the norm however and a review of the arrangement is therefore underway (as an integral part of the review of 'support roles' referred to above) with the objective of providing a practical solution which will withstand audit scrutiny.</p> <p>Risk levels are mitigated in that identified actions are being implemented and are on track to be completed within proposed timescales.</p>
<p>R2 A new Security Group is being created which include Audit, Business Support and ICT. This group will review the roles and access of the</p>	<p>Phil Burke</p>	<p>Established & work is on-going</p>	<p>A Security & Access working group has been established with a composition of ICT, Audit and Business Support staff. The group meet on a monthly basis and a Document Library has been established as the repository for a range of documents processed by the group (including review documents,</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provide By Service (Including Risks)
users. The group is currently being setup.			<p>processes, action plans, change requests, etc.).</p> <p>Reviews have been carried out relating to SAP Access Requests and 'Starter/Leaver' processes, etc. and improvements identified (e.g. the development of a computer program which automatically closes their SAP User account when a member of staff leaves the Council). Other reviews are proposed or in progress (e.g. a review of Segregation of Duties).</p> <p>No specific risks are identified in relation to this recommendation.</p>
<p>R3 We recommend that documentation of the SAP Security Policy is undertaken so that security administrators have appropriate understanding of security controls and procedures for SAP. A SAP Team Lead should also be appointed as soon as possible to ensure that all risks are appropriately managed and controlled. MCC will outsource the production of a SAP Security Policy. This will be completed within 3 months</p>	Phil Burke	April 2010	<p>In order to prime the development of a SAP Security Policy the Council's SAP software partner (HCL-Axon) has been commissioned to create a 'framework' policy document.</p> <p>This development work is in progress and should be complete by mid-December 2009. Once available, the framework policy document will need to be populated by MCC staff with details of existing procedures, controls, risk management, etc., and any gaps addressed.</p> <p>Since the original Audit, attempts have been made to recruit a SAP Security Architect / Team Lead but without success. A recent re-structure (Sept - Dec 2009) within the ICT Service however means that SAP Security & Assess staff have now been absorbed with a Technical Development team and there is no longer a specific post for a SAP Security Team Lead. Elements of risk may therefore result from the inability to recruit the necessary level of SAP security expertise. However there is a SAP Security Working Group (made up of staff from ICT / SAP Business Support team / Internal Audit),</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provide By Service (Including Risks)
			<p>which formally addresses SAP security issues and progresses issues to their resolution. Issues currently being addressed through the group include development of a SAP Security Policy / re-design of SAP Support roles / Reviews of security-related processes / Development of enhanced system functionality (e.g. automatic closure of user accounts when a member of staff leaves MCC's employment) / etc (this group meets once a month)</p>
<p>R4 The table containing the common passwords prohibited from use (Table USR40), should be populated and updated on a regular basis. This would help in maintaining active password control and limit the risk of unauthorised access into SAP. A new Change Request to implement that is being created. This should be implemented by the end of the year (December 2009).</p>	<p>Phil Burke</p>	<p>Complete 9 January 2010</p>	<p>With the exception of a relatively small number of system support staff, <u>all</u> end-users access SAP through the SAP Enterprise Portal where a Single Sign-on (SSO) regime is in place to the backend SAP systems. In this arrangement end-users need <u>only</u> authenticate themselves to the Portal using their Portal login/password. In contrast, table USR40 is a control available where users authenticate themselves directly to the backend SAP system and therefore the implementation of this table would <u>not</u> have the intended effect.</p> <p>To address the Audit concern, a decision has been taken to increase the strength of all Portal passwords by increasing the mandatory password length and also forcing use of special characters (*, &, %, etc ...) and a combination of upper & lower case content. This action will, in itself, discount the potential use of simple common words as end-user passwords.</p> <p>This new password regime will be introduced on January 9th. 2010.</p> <p>Risks are being mitigated significantly by the planned action of strengthening the SAP Portal password. This improvement may itself however be superceded in the foreseeable future should proposed moves take place to implement SSO to SAP</p>

Recommendation	Responsible Officer	Recommendation Completion Date	Assurance Provide By Service (Including Risks)
			using authentication against Active Directory.