East Hertfordshire District Council

Accounts Audit Approach Memorandum

June 2011

Our accounts audit approach

Introduction

This memorandum is intended to provides additional detail regarding our audit approach, as set out in our Audit Plan 2010/11 issued in November 2010, as well as an update on our response to key risks from the results of interim audit work carried out to date.

Audit approach reminder

We will:

- work closely with the finance team to ensure that we meet audit deadlines and conduct the audit efficiently
- plan our audit on an individual task basis at the start of the audit, and agree timetables with all staff involved; and
- consider the materiality of transactions when planning our audit and when reporting our findings

The logistical details of our annual accounts audit, as agreed with the Head of Financial Support Services, are detailed in Appendix A to this memorandum.

In summary our audit strategy comprises:

Planning	• Updating our understanding of the Council through discussions with management and a review of the management accounts
Control evaluation	• Reviewing the design effectiveness and implementation of internal financial controls including IT, where they impact the financial statements • Assessing audit risk and developing and implementing an appropriate audit strategy • Testing the operating effectiveness of selected controls • Assessing the effectiveness of internal audit against the CIPFA Code of Practice
Substantive procedures	• Reviewing material disclosure issues in the financial statements • Performing analytical review • Verifying all material income and expenditure and balance sheet accounts, taking into consideration whether audit evidence is sufficient and appropriate
Completion	• Performing overall evaluation • Determining an audit opinion • Reporting to Audit Committee

Our accounts audit approach (continued)

Materiality

An item would be considered material to the financial statements if, through it's omission or non-disclosure, the financial statements would no longer show a true or fair view.

Materiality is set at the outset of planning to ensure that an appropriate level of audit work is planned. It is then used throughout the audit process in order to assess the impact of any item on the financial statements. Any identified errors or differences greater than 2% of materiality will be recorded on a schedule of potential misstatements.

These are assessed individually and in aggregate, discussed with you and, if you do not adjust, signed off by you in your letter of representation to us, confirming your view that they are immaterial to the financial statements.

An item of low value may be judged material by its nature, for example any item that affects the disclosure of directors' emoluments. An item of higher value may be judged not material if it does not distort the truth and fairness of the financial statements.

Reliance on internal audit

We will work with the internal audit function to ensure our audit approach takes account of the risks identified and the work they have conducted, subject to our review of the effectiveness of the internal audit function.

Review of IT and outsourced systems

Our audit approach assumes that our clients use a computer system for accounting applications that process a large number of transactions. Accordingly, our approach requires a review of the Council's internal controls in the information technology (IT) environment.

We have involved Technology Risk Services (TRS) team members during the audit, this was based on the complexity of IT used in the significant transaction cycles and the control risk assessment.

Internal controls

Auditing standards require that we evaluate the design effectiveness of internal controls over the financial reporting process to identify areas of weakness that could lead to material misstatement. Therefore, we will focus our control review on the high risk areas of the financial statements.

We are also required to assess whether the controls have been implemented as intended. We will do this through a combination of inquiry and observation procedures, and, where appropriate, systems walkthroughs. However, our work cannot be relied upon necessarily to identify defalcations or other irregularities, or to include all possible improvements in internal control that a more extensive controls review exercise might identify.

Update on accounts audit risk assessment

As part of our planning and control evaluation work we have reviewed the audit risks identified in our Audit Plan 2010/11 and have set out opposite the outcome of work completed to date and further work planned.

Our updated review of the risks facing the Council has not identified any new risk areas.

We will report our full findings and conclusions in respect of each risk identified in our Annual Report to Those Charged with Governance (ISA 260) on completion of our final accounts audit.

Issue	Audit areas affected	Work completed	Further work planned
Accounting under IFRS	All areas of the financial statements	• A specific review of the Council's preparedness for IFRS has been completed. The results of this review have been reported to the Finance Team in a red/amber/green (RAG) format • We have maintained on-going liaison with the Finance Team regarding emerging IFRS issues and guidance has been provided for any proposed changes to accounting treatment being considered under IFRS	• We will continue to maintain on-going liaison with the Finance Team regarding emerging issues and new guidance released up until the signing of the 2010/11 financial statements • Our substantive audit procedures will focus on the high risk areas identified as a result of the transition to IFRS, in particular property, plant and equipment (PPE)
Financial performance pressures	All areas of the financial statements	• We have continued to monitor the Council's financial performance for the year against its agreed budget.	• We will continue to monitor the financial position of the council as well as reviewing the use of general reserves during the year. We will also carry out specific review on the Council's financial resilience in the light of SR10.

Update on accounts audit risk assessment (continued)

The specific accounts assertion risks by cycle which we consider to present a 'reasonably possible' risk of material misstatement to the financial statements are detailed in appendix B to this memorandum

Issue	Audit areas affected	Work completed	Further work planned
Revaluation of fixed assets	Property, plant and equipment	• System walkthroughs and controls testing have been undertaken in April to verify that controls relating to PPE activity and valuations are implemented and operating as expected.	• The use of valuation experts will be reviewed, to ensure that valuations have been completed in accordance with relevant IFRSs, in particular: - the appropriateness of data and instructions provided to the expert - the methods and assumptions applied by the expert
C3W project	All areas of the financial statements	• We have continued to monitor the progress with the C3W project.	• The C3W project is on-going and there continues to be a risk that such a significant change might impact on the delivery of objectives. • We will continue to monitor the progress of the project and consider any key impacts as they arise.

Results of interim audit work

Scope

As part of the interim audit work, and in advance of our final accounts audit fieldwork, we considered:

- the effectiveness of the Internal Audit function;
- internal audit's work on the Council's key financial systems;
- a review of closedown procedures in preparation for the final accounts under International Financial Reporting Standards (IFRS);
- walkthrough testing and tests of controls to confirm whether controls are implemented as per our understanding in areas where we have identified high accounting risk; and
- a review of Information Technology controls

The internal audit function

We review internal audit's overall arrangements against the 2006 CIPFA Internal Audit Standards. Where the arrangements are deemed to be adequate, we can gain assurance from the overall work undertaken by internal audit and can conclude that the service itself is contributing positively to the internal control environment and overall governance arrangements within the Council.

Overall, we have concluded that the Internal Audit service continues to provide an independent and satisfactory service to the Council and that we can take assurance from their work in contributing to an effective internal control environment at the Council.

In preparation for our final accounts audit, we sought to review internal audit's work on the financial systems.

In assessing the effectiveness of internal audit work, we reviewed three internal audit files to ensure that:

- systems were adequately documented;
- key controls have been identified and evaluated;
- key controls have been tested; and
- weaknesses have been reported to management

We were pleased to note from these files that no issues were identified with internal audit's work and these were produced to a high standard.

Closedown procedures

Our review considered the Council's timetable for closedown and the arrangements for preparing the draft IFRS accounts, including guidance provided on working papers required to be made available as part of the closedown process.

The Council has established a suitable timetable and expects to meet the accounts submission requirements in a timely manner. The Council also expects be able to provide detailed working papers to support the accounts at the start of our final accounts audit fieldwork, which is scheduled to commence on 8th August 2011, as well as providing the draft Annual Governance Statement in advance of this date.

Results of interim audit work (continued)

Walkthrough testing and tests of controls

Walkthrough tests and tests of controls were scheduled to be undertaken in April 2011 in relation to the specific accounts assertion risks by cycle which we consider to present a 'reasonably possible' risk of material misstatement to the financial statements. (These risks are detailed in Appendix B to this memorandum).

No significant issues were noted where walkthrough testing was able to be completed as planned and in-year internal controls were observed to operate satisfactorily in accordance with our documented understanding.

Review of information technology controls

Our information systems specialist performed a high level review of the general IT control environment, as part of the overall review of the internal controls system. We concluded that, from the work undertaken to date, there are no material weaknesses which are likely to adversely impact on the Council's financial statements.

We have, however, identified a number of areas for improvement during the course of our work in these areas. We do not consider these to pose a significant risk to the accounts. These have been covered opposite.

Implementation of previous years recommendations:

- Recommendations from our previous audit had not been implemented including security management reporting, formulation of security policies and procedures, review of privilege user accounts and IT risk management. In addition, we noted that work was being completed towards addressing weaknesses in business continuity and single point of failure risks
- Management should ensure that effective policy and procedures are developed to monitor and measure progress towards the implementation of agreed audit recommendations.

Security Management:

- Existing IT governance arrangements over IT security management are ineffective, as they fail to address roles, responsibilities and accountabilities for various aspects of security, including ownership.
- In the absence of effective governance over IT security, the infrastructure may be vulnerable to malicious exploitation.

Results of interim audit work (continued)

Vulnerability Assessment:

- We have been informed that a penetration test has been performed on the external facing network. However, we have found no evidence of any vulnerability results for the internal facing network and associated devices/configurations
- By not carrying out regular vulnerability assessments of the entire network infrastructure, potential threats and weaknesses may go undetected leading to potential malicious exploits that can have a direct impact upon the integrity of applications and data that utilise such resources.

User Account Management:

- The Council does not have any formal defined and documented policies and procedures for user account management. We have been informed that this is done on an ad hoc basis and notifications are not always received from Human Resources on a timely basis, especially when employees change roles within the Council.

Remote access:

- Remote access to the Council's network is granted to employees who work from home and third parties, for example software suppliers who maintain the Council's software applications. The Council has no formal documented policy in place for remote access. We have been advised that Human Resources keep records of all employees who permanently work from home either on a full time or part time basis. However, they do not hold such records for employees who work on an ad hoc basis.

Firewall Policy:

- A firewall policy should define how the Council's firewalls should handle inbound and outbound traffic and should be based on the existing security policies that stipulate requirements of the Council.
- We have been given assurance that a firewall configuration standard is in place but at the time of the audit we were not provided with a copy to review. In the circumstances we are unable to form an opinion on the effectiveness of such arrangements.

Appendices

A. Logistics

Timetables and milestones

The following proposed timetable and deadlines have been set and agreed with management:

Event	Date
Pre year end fieldwork including internal controls review	Mar-Apr 2011
Statutory accounts emailed to auditor	30 June 2011
Commence accounts audit fieldwork	8 August 2011
Manager visit to review work	August 2011
Partner visit to review work	August 2011
Clearance meeting to discuss our findings	August 2011
Report to Finance Audit and Risk Committee (ISA 260)	TBC

The audit process is underpinned by effective project management to ensure that we co-ordinate and apply our resources efficiently to meet your deadlines. It is therefore essential that we work closely with your team to achieve this timetable. An agreed format and schedule of informal update arrangements will be maintained throughout the course of our audit fieldwork in support of this aim.

Engagement team

In accordance with our Audit Plan 2010/11 issued February 2011, the main engagement team for the accounts audit will include:

Name	Role	Contact details
Paul Dossett	Engagement partner	T: 0207 728 3180 E: paul.dossett@uk.gt.com
Nick Taylor	Audit manager	T: 07500 815358 E: nick.taylor@uk.gt.com
Simon Cooke	Audit senior	T: 0207 728 2790 E: simon.j.cooke@uk.gt.com

Information requirements

The information and working paper requirements that would assist us in an efficient and timely audit of the year-end financial statements have been communicated to the finance team within our Arrangements Letter, which was issued in March 2011.

B. Accounts assertion risks by cycle

A reasonably possible risk is defined as being where:

- Numerous and often very precise controls should be established by management
- Substantive procedures would vary if controls were tested
- Inherent risk factors increase the likelihood of a material misstatement

Property, plant and equipment

Valuation - Gross

Risks	Intended control reliance
Property, plant and equipment activity not valid	Tests of controls will be performed to verify that controls operate effectively
Revaluation measurements not correct	Walkthroughs will be performed to verify that controls are implemented

Valuation - Net

Risks	Intended control reliance
Allowance for depreciation not adequate	Walkthroughs will be performed to verify that controls are implemented

Operating expenses

Completeness

Risks	Intended control reliance
Creditors understated or not recorded in correct period	Walkthroughs will be performed to verify that controls are implemented

Council Tax Revenue / NNDR Revenues

Completeness

Risks	Intended control reliance
Tax revenue transactions not recorded	Walkthroughs will be performed to verify that controls are implemented

Existence/Occurrence

Risks	Intended control reliance
Recorded debtors not valid	Walkthroughs will be performed to verify that controls are implemented

Valuation - Net

Risks	Intended control reliance
Allowance for doubtful accounts not adequate	Walkthroughs will be performed to verify that controls are implemented

Grant Revenues

Existence/Occurrence

Risks	Intended control reliance
Recorded debtors not valid	Walkthroughs will be performed to verify that controls are implemented

C. Action plan

Rec No.	Recommendation	Priority	Management Comments	Implementation date and responsibility
IT recommendations				
1	Management should ensure that regular vulnerability assessments are carried out over the entire network estate, both internal and external facing, to identify potential risks so that these can be eliminated or mitigating controls put in place.	**H**		
2	Management should introduce improvements to existing governance arrangements by way of the IT Steering Group, which is tasked with addressing all IT security matters, including the formulation of corporate policy and procedures.	**M**		
3	Management should ensure that a user account management policy is established with related procedures and templates to ensure consistency in user set ups, modifications and deletion. This should also include privilege user accounts.	**M**		
4	Management should ensure that a documented policy is in place for remote access.	**M**		
5	Management should ensure that a corporate firewall is defined, documented and enforced that makes reference to pertinent procedures and baseline technical security configuration standards.	**M**		

www.grant-thornton.co.uk