

Audit Committee – 20 July 2015

External Auditor's Audit Plan Report 2014/15

1. Summary of report

- 1.1 This report contains the external auditors Audit Plan 2014/15 providing details regarding Grant Thornton's audit approach for the 2014/15 Statement of Accounts along with the results of their interim audit work to date, recommendations arising from this and the Council's response.

2. Recommendations

- 2.1 Audit Committee is requested to note the report and the measures being taken to ensure the council meets its obligations.

3. Governance

- 3.1 Each year the council's external auditors report to the Audit Committee on their approach to their audit of the annual accounts and the results of their interim audit of the accounts. The report highlights several recommendations and includes the council's response to these.

4. Resource and legal considerations

- 4.1 None directly relating to this report.

5. Performance and risk management issues

- 5.1 Performance and risk management is embedded in the final accounts process.

6. Equality implications

- 6.1 None directly associated with this report.

7. Consultation

- 7.1 The report is prepared in consultation with finance and senior officers across the council.

8. Background papers - Various financial working papers.

Author: Vicky Buckley – Head of Finance, ☎ 01922 652326, buckleyv@walsall.gov.uk



James Walsh, Chief Finance Officer
1 July 2015

The Audit Plan for Walsall Metropolitan Borough Council

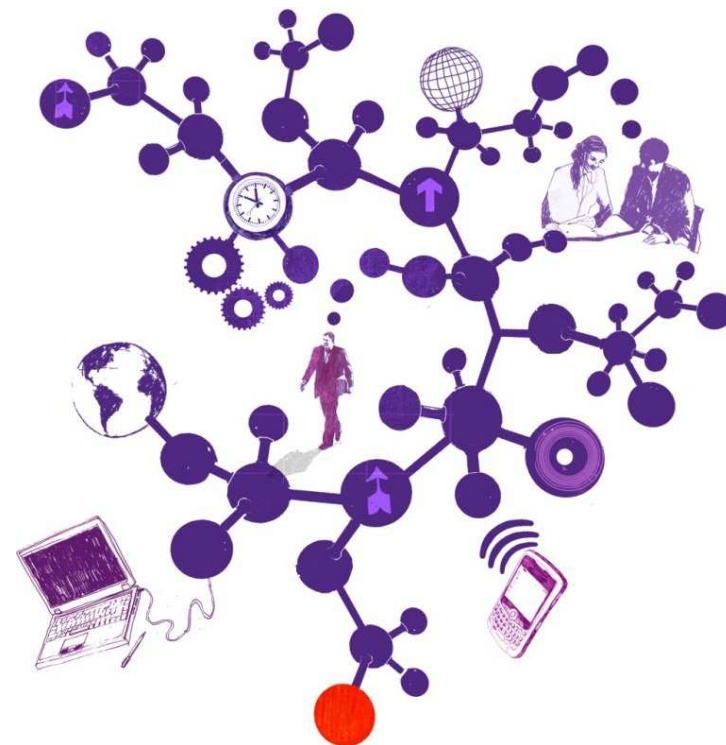
Year ended 31 March 2015

July 2015

Jon Roberts
Partner
T 0121 232 5410
E jon.roberts@uk.gt.com

Nicola Coombe
Audit Manager
T 0121 232 5206
E nicola.coombe@uk.gt.com

Zoe Thomas
Audit Manager
T 0121 232 5277
E zoe.thomas@uk.gt.com



Contents

Section

1. Understanding your business	3
2. Developments relevant to your business and the audit	4
3. Our audit approach	5
4. Significant risks identified	6
5. Other risks	7
6. Value for Money	9
7. Results of interim work	10
8. Key dates	12
9. Fees and independence	13
10. Communication of audit matters with those charged with governance	14
11. Appendix 1 – IT findings and Management response	

The contents of this report relate only to the matters which have come to our attention, which we believe need to be reported to you as part of our audit process. It is not a comprehensive record of all the relevant matters, which may be subject to change, and in particular we cannot be held responsible to you for reporting all of the risks which may affect the Council or any weaknesses in your internal controls. This report has been prepared solely for your benefit and should not be quoted in whole or in part without our prior written consent. We do not accept any responsibility for any loss occasioned to any third party acting, or refraining from acting on the basis of the content of this report, as this report was not prepared for, nor intended for, any other purpose.

Understanding your business

In planning our audit we need to understand the challenges and opportunities the Council is facing. We set out a summary of our understanding below.

Challenges/opportunities

1. Procurement and Commissioning

- In the Council strategic plan you recognise that the Council will need to focus on priorities and provide services differently. This may involve working with partners and considering alternative delivery methods.

2. LG Reorganisation

- The go ahead has recently been given on the West Midlands Combined Authority. The full implications for the council are far from clear. It is hoped that this will provide opportunities to improve services for example, through better integration of health and social care and encourage investment in the area, promoting improved economic prosperity and growth.

3. LG Finance Settlement

- The local government spending settlement showed local authorities are facing a cash reduction in their spending power of up to 6% in 2015/16. Walsall is facing a reduction of 3.8%.
- At the same time local authorities are facing increasing demands for school places and adult social care services.
- Walsall is currently forecasting a need to save £82m over the next 4 years.

4. Collaborative working with the NHS.

- Walsall has agreed a BCF plan and established a pooled budget (section 75 agreement) with Walsall CCG. Total contributions to the pooled fund will be C £21.5million by the CCG and £2.5m by the Council.

5. Looked after children in Walsall

- There are over 600 looked after children in Walsall. This level of demand, it puts strain on the Council's finances. The overspend on LAC and agency workers in children's services is £4.6m.

Our response

- We will review the progress you have made in delivering your efficiency savings in this area as part of our work on your arrangements for financial resilience.
- we will discuss with you your plans for restructuring services and provide a view where considered to be appropriate.

- We will discuss your plans in these areas through our regular meetings with senior management and those charged with governance, providing a view where appropriate.

- We will review your Medium Term Financial Plan and financial strategy as part of our work on your arrangements for financial resilience.

- We will discuss your plans in these areas through our regular meetings with senior management and those charged with governance, providing a view where appropriate.

Through discussions with key staff and document review we will evaluate the impact of the Council's plans to monitor and react to the financial risks identified. We will also follow up the Council's progress following the Ofsted inspection.

Developments relevant to your business and the audit

In planning our audit we also consider the impact of key developments in the sector and take account of national audit requirements as set out in the Code of Audit Practice ('the code') and associated guidance.

Developments and other requirements

1. Financial reporting

- Changes to the CIPFA Code of Practice.
- Changes to the recognition of school land and buildings on local authority balance sheets.

2. Legislation

- Local Government Finance settlement.

3. Corporate governance

- Annual Governance Statement (AGS).
- Explanatory foreword.

4. Financial Pressures

- Managing service provision with less resource.
- Progress against savings plans.

5. Other requirements

- The Council is required to submit a Whole of Government accounts pack on which we provide an audit opinion.
- The Council completes a grant claim on which audit certification is required.

Our response

We will ensure that

- The Council complies with the requirements of the CIPFA Code of Practice through discussions with management and our substantive testing.
- Schools are accounted for correctly and in line with the latest guidance.

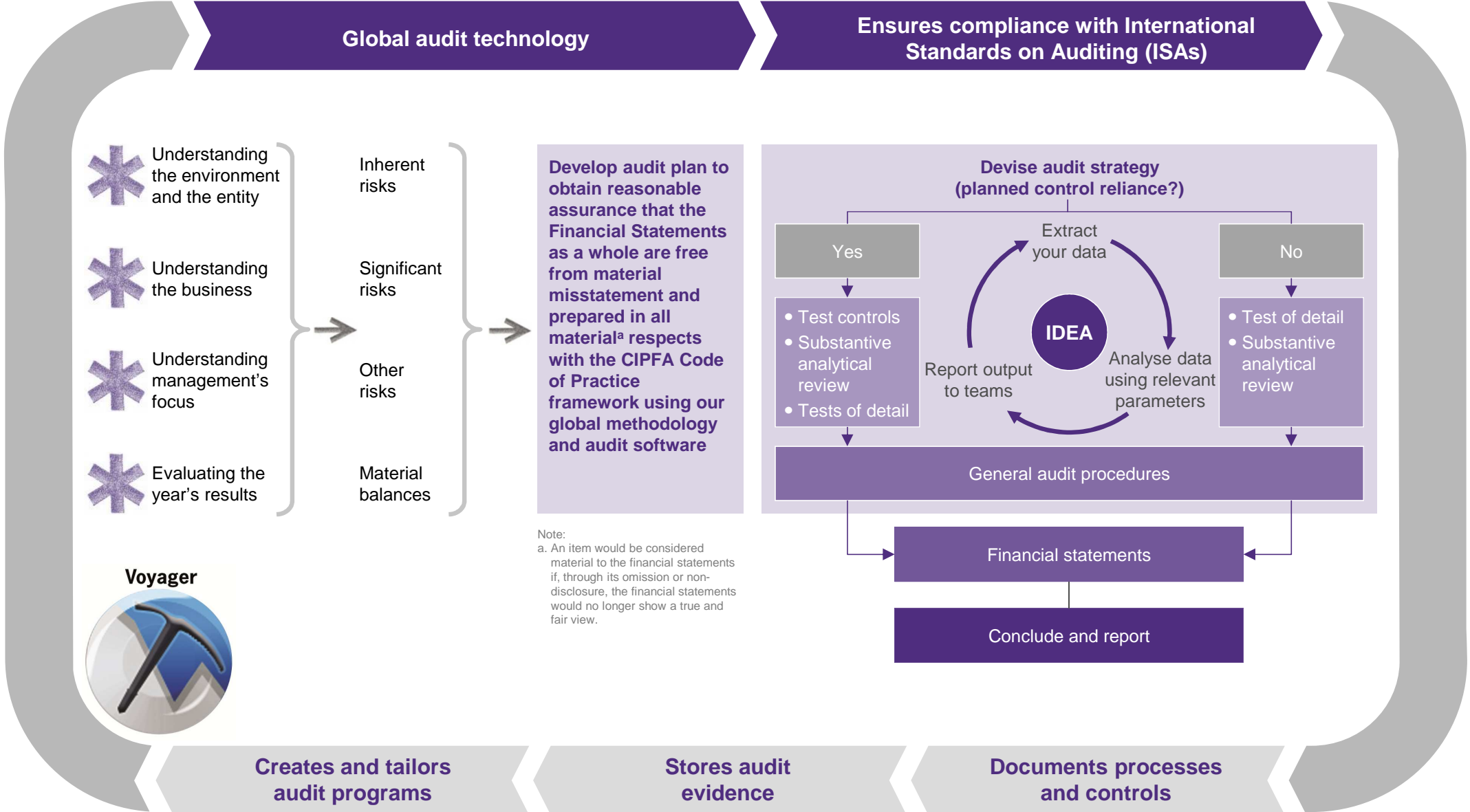
- We will discuss the impact of the legislative changes with the Council through our regular meetings with senior management and those charged with governance, providing a view where appropriate.

- We will review the arrangements the Council has in place for the production of the AGS.
- We will review the AGS and the explanatory foreword to consider whether they are consistent with our knowledge.
- We will continue to discuss with you local governance issues including regularisation of appointments.

- We will review the Council's performance against the 2014/15 budget, including consideration of performance against the savings plan.
- We will undertake a review of Financial Resilience as part of our VfM conclusion.

- We will carry out work on the WGA pack in accordance with requirements.
- We will certify the housing benefit subsidy claim in accordance with the requirements specified by Public Sector Audit Appointments Ltd. This company will take over the Audit Commission's responsibilities for housing benefit grant certification from 1 April 2015.

Our audit approach



Significant risks identified

'Significant risks often relate to significant non-routine transactions and judgmental matters. Non-routine transactions are transactions that are unusual, either due to size or nature, and that therefore occur infrequently. Judgmental matters may include the development of accounting estimates for which there is significant measurement uncertainty' (ISA 315).

In this section we outline the significant risks of material misstatement which we have identified. There are two presumed significant risks which are applicable to all audits under auditing standards (International Standards on Auditing – ISAs) which are listed below:

Significant risk	Description	Substantive audit procedures
The revenue cycle includes fraudulent transactions	<p>Under ISA 240 there is a presumed risk that revenue may be misstated due to the improper recognition of revenue.</p> <p>This presumption can be rebutted if the auditor concludes that there is no risk of material misstatement due to fraud relating to revenue recognition.</p>	<p>Having considered the risk factors set out in ISA240 and the nature of the revenue streams at the Council, we have determined that the risk of fraud arising from revenue recognition can be rebutted, because:</p> <ul style="list-style-type: none"> • there is little incentive to manipulate revenue recognition • opportunities to manipulate revenue recognition are very limited • the culture and ethical frameworks of local authorities, including WMBC, mean that all forms of fraud are seen as unacceptable.
Management over-ride of controls	Under ISA 240 the presumption that the risk of management over-ride of controls is present in all entities.	<p>Work completed to date:</p> <ul style="list-style-type: none"> • Review of accounting estimates, judgments and decisions made by management • Testing of journal entries • Review of unusual significant transactions <p>Further work planned:</p> <ul style="list-style-type: none"> • Review of accounting estimates, judgments and decisions made by management • Testing of journal entries • Review of unusual significant transactions

Other risks identified

The auditor should evaluate the design and determine the implementation of the entity's controls, including relevant control activities, over those risks for which, in the auditor's judgment, it is not possible or practicable to reduce the risks of material misstatement at the assertion level to an acceptably low level with audit evidence obtained only from substantive procedures (ISA 315).

In practise this means we make a judgment which systems are the most at risk of material misstatement and undertake additional non- substantive procedures. Factors considered include the complexity, volume and materiality of transactions in those systems. Additional procedures include documenting key controls and undertaking walkthroughs to confirm the operation of controls in line with our understanding. We also make a judgement which aspect of the system presents the most risk – for example completeness of transactions and design appropriate procedures to address that risk.

In this section we outline the other risks of material misstatement which we have identified as a result of our planning.

Other risks	Description	Work completed to date	Work to be performed
Operating expenses	Creditors understated or not recorded in the correct period (completeness)	<ul style="list-style-type: none"> We have documented our understanding of the processes and key controls over the transaction cycle Walkthrough tests were completed in relation to the completeness assertion, to assess whether those controls are designed effectively Early testing of operating expenses throughout the year (testing to be completed at final accounts) We have also reviewed the revised basis of the MRP and have concluded that we are unlikely to challenge the approach, provided that Members are satisfied that a prudent approach is being taken. 	<p>Further work planned:</p> <ul style="list-style-type: none"> Cut off testing of purchase orders and goods received notes Review of the completeness of the year end reconciliation to the purchasing system. Testing for unrecorded liabilities
Employee remuneration	Employee remuneration and benefit obligations and expenses understated (completeness)	<ul style="list-style-type: none"> We have documented our understanding of the processes and key controls over the transaction cycle Walkthrough tests were completed in relation to the completeness assertion, which we consider to present a risk of material misstatement to the financial statements. Sample testing of employee remuneration expenditure throughout the year to underlying records (testing to be completed at final accounts) 	<ul style="list-style-type: none"> Tests of detail on the employee remuneration accrual and tax obligation, if material Review of the completeness of the payroll reconciliation to ensure that the payroll information is consistent with the ledger and financial statements Monthly trend analysis of payments made through the payroll system. Agreement of employee remuneration disclosures in the financial statements to supporting evidence

Other risks identified (significant)

The auditor should evaluate the design and determine the implementation of the entity's controls, including relevant control activities, over those risks for which, in the auditor's judgment, it is not possible or practicable to reduce the risks of material misstatement at the assertion level to an acceptably low level with audit evidence obtained only from substantive procedures (ISA 315).

In this section we outline the other risks of material misstatement which we have identified as a result of our planning.

Other significant risks	Description	Work completed to date	Work to be performed
Birmingham Airport Shares.	The Council holds both ordinary and preference shares in BAH Ltd along with six other West Midlands authorities. Over the last year, the value of this investment is expected to increase.	None to date.	Grant Thornton valuation specialists will undertake a review of the share valuation report to ensure appropriate disclosure in the Council's financial statements.

Value for money

Value for money

The Code requires us to issue a conclusion on whether the Council has put in place proper arrangements for securing economy, efficiency and effectiveness in its use of resources. This is known as the Value for Money (VfM) conclusion.

Our VfM conclusion is based on the following criteria specified by the Audit Commission:

VfM criteria	Focus of the criteria
The organisation has proper arrangements in place for securing financial resilience	The organisation has robust systems and processes to manage financial risks and opportunities effectively, and to secure a stable financial position that enables it to continue to operate for the foreseeable future
The organisation has proper arrangements for challenging how it secures economy, efficiency and effectiveness	The organisation is prioritising its resources within tighter budgets, for example by achieving cost reductions and by improving efficiency and productivity

We have undertaken a risk assessment to identify areas of risk to our VfM conclusion. We will undertake work in the following areas to address the risks identified:

- Emerging corporate plan and financial strategy; the level of savings that the Council will need to deliver in the next 4 years are considerable.
- Social Care and inclusion (SCI) and children's services directorates continuing overspends.
- School attainment; Ofsted has highlighted that arrangements for supporting school improvement are ineffective.

The results of our VfM audit work and the key messages arising will be reported in our Audit Findings report and in the Annual Audit Letter.

Results of interim audit work

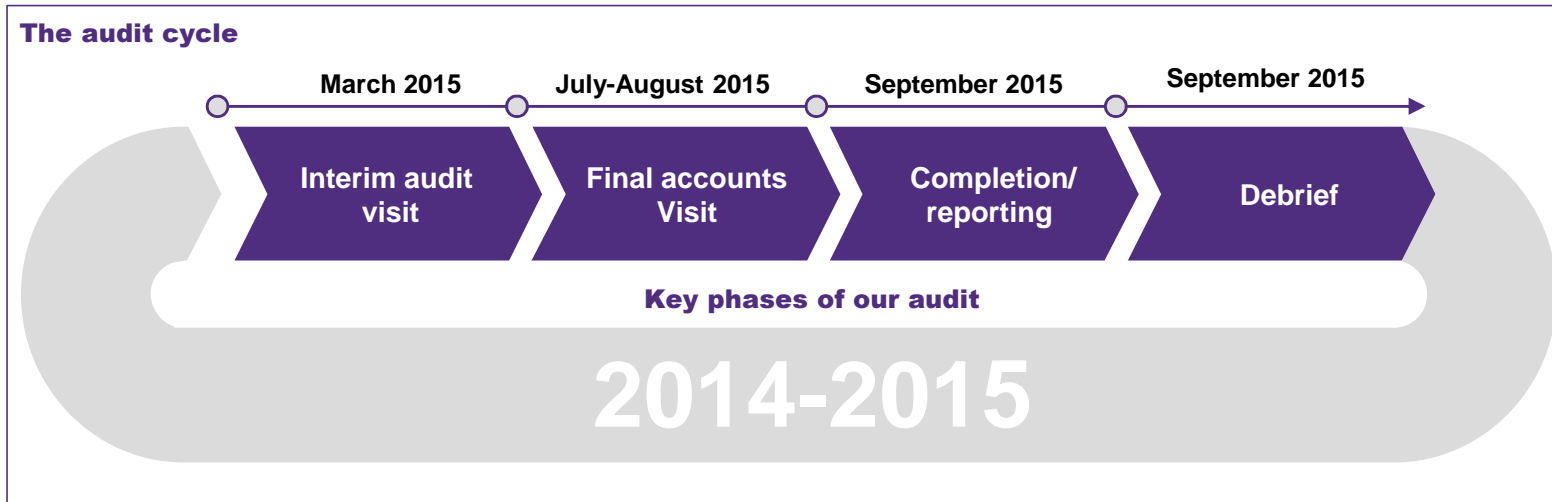
The findings of our interim audit work, and the impact of our findings on the accounts audit approach, are summarised in the table below:

	Work performed and findings	Conclusion
Internal audit	<p>We have completed a high level review of internal audit's overall arrangements. Our work has not identified any issues which we wish to bring to your attention.</p> <p>We also reviewed internal audit's work on the Council's key financial systems to date. We have not identified any significant weaknesses impacting on our responsibilities.</p>	<p>We have concluded that internal audit's responsibilities are appropriate and they have appropriate status within the authority. Internal audit has adopted appropriate methods for undertaking their work and their plan includes coverage of internal controls, including financial, and consideration of governance issues. They report their findings effectively and are able to report independently to Audit Committee.</p> <p>Our review of internal audit work has not identified any weaknesses which impact on our assessment of the control environment.</p> <p>As part of our final accounts visit we will review those internal audit reports that have been finalised and take account where applicable of any impact on our audit approach.</p>
Walkthrough testing	<p>We have completed walkthrough tests of controls operating in areas where we consider that there is a risk of material misstatement to the financial statements.</p> <p>Our work has not identified any issues which we wish to bring to your attention. Internal controls have been implemented in accordance with our documented understanding.</p>	<p>Our work has not identified any weaknesses which impact on our audit approach on the core financial systems.</p>
Entity level controls	<p>We have obtained an understanding of the overall control environment relevant to the preparation of the financial statements including:</p> <ul style="list-style-type: none"> • Communication and enforcement of integrity and ethical values • Commitment to competence • Participation by those charged with governance • Management's philosophy and operating style • Organisational structure • Assignment of authority and responsibility • Human resource policies and practices 	<p>Our work has identified no material weaknesses which are likely to adversely impact on the Council's financial statements. Weakness at an entity level has been identified as part of our IT review (see over).</p>

Results of interim audit work cont'd

	Work performed	Conclusion
Review of information technology controls	<p>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 have also performed a follow up of the issues that were raised last year.</p> <p>IT (information technology) controls were observed to have been implemented in accordance with our documented understanding.</p>	<p>Our work has identified weakness in internal controls. These and management responses are reported in Appendix 1. Management responses in the Appendix have been considered by our IT lead and judged to be appropriate. We are currently assessing the impact on our testing strategy, although the nature of the weaknesses identified are such that it is likely that our planned substantive procedures and journal testing should provide us with sufficient assurance that the accounts are not materially misstated, without undertaking significant additional work.</p> <p>Whilst these matters do present a risk of error and fraud occurring and should be addressed, it is likely that other factors would need to be present for a material fraud to occur or to not be identified. Collusion and / or failure in other financial and operational controls would in most cases need to be present. The work of internal audit has not identified any significant weakness in the operation of key financial systems or budgetary control arrangements and our walk-throughs and other planning procedures have not identified the absence of expected controls or procedures.</p>
Journal entry controls	<p>We have reviewed the Council's journal entry policies and procedures as part of determining our journal entry testing strategy and have not identified any material weaknesses which are likely to adversely impact on the Council's control environment or financial statements.</p> <p>Testing on journal transactions recorded in the financial year 2014/15 will be tested during the final accounts audit.</p>	<p>We noted that the roles of senior financial reporting managers include the ability to post journals. We will address this risk through targeting such journals and testing them to underlying records.</p>
Property Plant and Equipment	<p>We have undertaken some early substantive testing so that we can reduce the volume of testing required at final accounts. This work has included:</p> <ul style="list-style-type: none"> • testing of additions to underlying documentation – no issues from testing to date. Further testing to be undertaken post statements. • Testing of disposals. • Review of PFI. • Review of the principles surrounding accounting for schools. 	<p>We have yet to fully conclude on this work as we need to complete testing for the full financial year. However there are no matters that we need to bring to your attention at this stage.</p>

Key dates



Date	Activity
January 2015	Planning
March 2015	Interim site visit
July 2015	Presentation of audit plan to Audit Committee
July-August 2015	Year end fieldwork
w/c 7 September 2015	Audit findings clearance meeting with Director of Finance
24 September 2015	Report audit findings to those charged with governance (Audit Committee/Board)
September 2015	Sign financial statements opinion

Fees and independence

Fees

	£
Council audit	189,000
Grant certification	19,210
Total fees (excluding VAT)	208,210

Our fee assumptions include:

- Supporting schedules to all figures in the accounts are supplied by the agreed dates and in accordance with the agreed upon information request list
- The scope of the audit, and the Council and its activities, have not changed significantly
- The Council will make available management and accounting staff to help us locate information and to provide explanations

Grant certification

- Our fees for grant certification cover only housing benefit subsidy certification, which falls under the remit of Public Sector Audit Appointments Limited, as the successor to the Audit Commission in this area.
- Fees in respect of other grant work, such as reasonable assurance reports, are shown under 'Fees for other services.'

Fees for other services

Service	Fees £
2013/ 14 Governance Review (fees charged this year)	5,500
Teachers Pension Certification	4,200

Fees for other services

Fees for other services reflect those agreed at the time of issuing our Audit Plan. Any changes will be reported in our Audit Findings Report and Annual Audit Letter.

Independence and ethics

We confirm that there are no significant facts or matters that impact on our independence as auditors that we are required or wish to draw to your attention. We have complied with the Auditing Practices Board's Ethical Standards and therefore we confirm that we are independent and are able to express an objective opinion on the financial statements.

Full details of all fees charged for audit and non-audit services will be included in our Audit Findings report at the conclusion of the audit.

We confirm that we have implemented policies and procedures to meet the requirement of the Auditing Practices Board's Ethical Standards.

Communication of audit matters with those charged with governance

International Standards on Auditing (ISA) 260, as well as other ISAs, prescribe matters which we are required to communicate with those charged with governance, and which we set out in the table opposite.

This document, The Audit Plan, outlines our audit strategy and plan to deliver the audit, while The Audit Findings will be issued prior to approval of the financial statements and will present key issues and other matters arising from the audit, together with an explanation as to how these have been resolved.

We will communicate any adverse or unexpected findings affecting the audit on a timely basis, either informally or via a report to the Council.

Respective responsibilities

This plan has been prepared in the context of the Statement of Responsibilities of Auditors and Audited Bodies issued by the Audit Commission (www.audit-commission.gov.uk).

We have been appointed as the Council's independent external auditors by the Audit Commission, the body responsible for appointing external auditors to local public bodies in England. As external auditors, we have a broad remit covering finance and governance matters.

Our annual work programme is set in accordance with the Code of Audit Practice ('the Code') issued by the Audit Commission and includes nationally prescribed and locally determined work. Our work considers the Council's key risks when reaching our conclusions under the Code.

It is the responsibility of the Council to ensure that proper arrangements are in place for the conduct of its business, and that public money is safeguarded and properly accounted for. We have considered how the Council is fulfilling these responsibilities.

Our communication plan	Audit plan	Audit findings
Respective responsibilities of auditor and management/those charged with governance	✓	
Overview of the planned scope and timing of the audit. Form, timing and expected general content of communications	✓	
Views about the qualitative aspects of the entity's accounting and financial reporting practices, significant matters and issue arising during the audit and written representations that have been sought		✓
Confirmation of independence and objectivity	✓	✓
A statement that we have complied with relevant ethical requirements regarding independence, relationships and other matters which might be thought to bear on independence.	✓	✓
Details of non-audit work performed by Grant Thornton UK LLP and network firms, together with fees charged.		
Details of safeguards applied to threats to independence		
Material weaknesses in internal control identified during the audit		✓
Identification or suspicion of fraud involving management and/or others which results in material misstatement of the financial statements		✓
Non compliance with laws and regulations		✓
Expected modifications to the auditor's report, or emphasis of matter		✓
Uncorrected misstatements		✓
Significant matters arising in connection with related parties		✓
Significant matters in relation to going concern		✓

Appendix 1

Key to assessment of internal control deficiencies


- Material weakness –risks of material misstatement
- significant deficiency – risk of significant misstatement
- Deficiency – risk of inconsequential misstatement

	Assessment	Issue and risk	Recommendation
1	●	<p>Default Oracle passwords have not been changed</p> <p>Oracle E-Business Suite and Oracle RDBMS ship with a number of out of the box accounts that have system administrator privileges. Our testing identified that Walsall MBC have an E-Business Suite account (OP_SYSADMIN) that has not had the default password changed. This account has the 'system administrator' responsibility assigned to it, the highest level of access within E-Business Suite.</p> <p>We also identified one high-risk Oracle database account that has not had the default password changed (CTXSYS). This account is a privileged database account that allows the creation of users and the assigning of access rights, and therefore effectively has system administration rights. We also identified a further 21 lower risks database accounts that have not had their default passwords changed.</p> <p><u>This condition presents the following risk to the organisation:</u> Default accounts present a security risk as the usernames and passwords are widely available. They therefore present an easy point of compromise for a malicious user who could use such an account to create new user accounts and assign unauthorised privileges to them. These accounts could then be used to perform unauthorised and unaccountable changes or transactions, providing an easy method of committing fraudulent activity. Management should also note that default accounts are anonymous and any inappropriate or legitimate actions carried out by them undermine the concept of non-repudiation.</p>	<p>Default passwords should be changed immediately to avoid the risk of system compromise.</p> <p>Management should ensure that for any future upgrades or developments a thorough review of shipped accounts is undertaken and all default passwords changed.</p> <p>Management response: E-Business suite account OP_SYSADMIN default password has been changed with a mandatory 60 days password change added. <i>Implemented 6.05.2015.</i> <i>Jane Hanslip, Senior Financial Admin Officer, Financial Administration</i> We are in consultation with Version one to implement a password refresh procedure that will not compromise any system database activities but limit the risk of unauthorised access. This will need to be a controlled implementation through development and test environments to ensure successful promotion to the live environment. <i>Implementation 30.06.2015</i> <i>Jane Hanslip, Senior Financial Admin Officer, Financial Administration.</i></p>

Appendix 1

	Assessment	Issue and risk	Recommendation
2	●	<p>Responsibility with 'processes tab' functionality</p> <p>The 'processes tab' (also known as 'AZN menus') is a known security risk present within Oracle E-Business Suite. It is used for system developers during the implementation stage to easily configure business workflows and should not be enabled within the production environment. The processes tab displays workflows diagrammatically, however it also enables the related functions to be performed, bypassing the responsibilities allocated to a user. For example a user with the out of the box responsibility 'Payables Manager' can view the accounts payable workflow on the processes tab. This will also enable the user to perform any of these stages, such as making a payment. AZN menus are linked to a responsibility and provide privileged access to the functional area of the responsibility.</p> <p>We acknowledge that Walsall MBC have removed the AZN menus from most responsibilities, however our review identified that the responsibility 'WMBC Payables Manager Suppliers' still contains this functionality. The purchase to pay process is considered to be a high risk function and therefore presents a potential fraud risk.</p> <p><u>This condition presents the following risk to the organisation:</u></p> <p>Users are able to have unsegregated access to the whole accounts payable process. Given the relative obscurity of the AZN 'backdoor' it is probable that financial management are not aware of the risks involved and may not have sufficient compensating controls in place to detect payables fraud.</p>	<p>The AZN menus should be excluded from the 'WMBC Payables Manager Suppliers' responsibility.</p> <p>Management response:</p> <p>This has now been removed. Implemented 6.05.2015. Segregation of duties built into the payment process prevents unauthorised transactions being made. The cheque print process is carried out by various teams to ensure segregation of duties and prevent possible fraudulent activities. The cheque printing is carried out by a different department to the department processing the payment. the cheques are then collected by another department and reconciled back to a report sent by the team processing the payment. For bacs payments there is a separate software used to send these payments and individual secure bacs software cards to transfer bacs. All payments are reconciled on a daily basis and a transfer of funds from the general account to the bacs account is authorised and completed via business internet banking. This is then authorised on line with secure business internet banking cards assigned to individuals from a different department (finance). the users with 'WMBC payables Manager Suppliers' do not have access to the bacs software, they are not assigned the secure bacs software cards or allowed access to cheque stationery or the printing of cheques. These users are not set up to access business internet banking or release funds.</p> <p><i>Implemented 6.05.2015.</i></p> <p><i>Jane Hanslip, Senior Financial Admin Officer, Financial Administration.</i></p>

Appendix 1

	Assessment	Issue and risk	Recommendation
3		<p>Use of generic accounts</p> <p>We identified two generic accounts (CORPORATEBUYER and PROCUREMENT) that have default responsibilities assigned to them. Default responsibilities allow unsegregated access to functions within Oracle E-Business Suite, allowing a user to exploit the 'processes tab' vulnerability. The PROCUREMENT account was last logged in to on as recently as 30/12/2014.</p> <p><u>This condition presents the following risk to the organisation</u> Fraudulent or inappropriate transactions cannot be linked to individuals due to the use of generic accounts.</p>	<p>The use of default responsibilities should be ceased, especially those that are assigned to generic accounts, as these present the greatest risk of misuse.</p> <p>Management Response:</p> <p>The generic accounts CORPORATEBUYER and PROCUREMENT are only accessed by one user to view notifications that have escalated to the buffer zone. Both generic accounts will be ceased.</p> <p><i>Implement 12.06.2015. Jane Hanslip, Senior Financial Admin Officer, Financial Administration</i></p>

Appendix 1

	Assessment	Issue and risk	Recommendation
4	●	<p>Oracle Support Administrator responsibility</p> <p>WMBC have built a custom responsibility for second-line support ('Oracle Support Administrator'). These users are responsible for support requests such as password resets. The 'Oracle Support Administrator' responsibility allows access to the 'Users' form. Access to this form effectively allows full system administrator functionality, as a user can assign any responsibility to themselves or change the password on the SYSADMIN account. There is therefore a relatively large number of users with system administrator responsibilities (26).</p> <p><u>This condition presents the following risk to the organisation</u></p> <p>Whilst it is acknowledged that WMBC have a control in place to review audit logs on a monthly basis, users may assign themselves unauthorised access rights and have the possibility to delete audit trails.</p>	<p>Management should review the existing arrangements for first line support with a view to reducing the number of users that have access to the 'Users' form, for example through the implementation of password self-service as part of the planned upgrade to r12.</p> <p>Management may also consider a coding change for the form to prevent users assigning all privileges.</p> <p>Management response:</p> <p>The number of users with system administrator responsibilities will be reviewed with immediate effect and reduced where necessary. Furthermore, with the introduction of password self service in R12 (user clicks on the forgotten password option, enters their email address and a temporary password is sent to them via email in order to log onto Oracle. Oracle will then ask the user to create a new password) the number of users will reduce further.</p> <p>As detailed there are audit logs reviewed every month on changes to user access. However, in addition to this every process from supplier set up, amendment of supplier records, purchase order approval, invoice entry, pre payment checks, payment transfers, cheque printing, bacs transfers, payment reconciliations has independent checks and segregation of duties in place to mitigate any risks. Accounts Receivable customer set up, raising of invoices all have independent checks and segregation of duties in place, again to mitigate any risks.</p> <p>Review of current System administrator users - agreed – 12.06.2015. R12 implementation of password self serve go live 1st October 2015</p>

Jane Hanslip, Senior Financial Admin Officer, Financial Administration

Appendix 1

	Assessment	Issue and risk	Recommendation
5	●	<p>Users self-assigning responsibilities</p> <p>There have been four instances in the year under review where users have assigned themselves additional responsibilities in Oracle EBS. It is WMBC policy that any additional responsibilities should be approved, even if this is retrospectively should an emergency fix be required. This had been performed for those occasions when a user had self-assigned themselves a responsibility in the current year. However, there is no requirement for responsibilities to be end-dated.</p> <p><u>This condition presents the following risk to the organisation</u></p> <p>User access have access rights in excess of those they require to perform their role, increasing the risk of unauthorised access or functions being performed.</p>	<p>All additional responsibilities that users assign themselves must be end-dated, this information should be recorded on the existing authorisation spreadsheet and periodic monitoring undertaken to ensure that users do not remain with access rights they do not require.</p> <p>Management response:</p> <p><i>Agreed – Implemented 06.05.2015 – Jane Hanslip, Senior Financial Admin Officer – Financial Administration</i></p>

Appendix 1

	Assessment	Issue and risk	Recommendation
6	●	<p>Users with ability to execute SQL code</p> <p>There are currently 17 user accounts on the system that have access to an Oracle form or function that allows the execution of SQL code directly against the database. These users are mainly located within the Oracle support team, however there are also two generic accounts (refer to ' Use of generic accounts ') that have this functionality.</p> <p><u>This condition presents the following risk to the organisation</u></p> <p>A user could use modify data within the application through the use of SQL code to commit fraud, for example the modification of supplier standing data. It is acknowledged that this presents a relatively low level of risk due to the degree of knowledge that would be required to use SQL code to bypass internal controls and/or commit fraudulent / unauthorised activities.</p>	<p>Responsibilities that have forms and functions assigned to them that enable the execution of SQL code should be reviewed to ensure that they are available only to those members of staff who strictly require it.</p> <p>Management response: Challenge recommendation:- The forms and functions that enable the execution of SQL code will be removed. This represents a higher level of control than recommended.</p> <p><i>12.06.2015 – Jane Hanslip. Senior Financial Admin Officer – Financial Administration</i></p>

Appendix 1

	Assessment	Issue and risk	Recommendation
7	●	<p>Proactive reviews of logical access within Northgate Rev & Bens and Active Directory</p> <p>User accounts and associated permissions within Northgate Rev & Bens and Active Directory are not formally, proactively reviewed for appropriateness.</p> <p>This issue was identified as a finding in the 2013-14 audit, the rating of the finding has been escalated in reflection of it not being addressed.</p> <p><u>This condition presents the following risk to the organisation</u></p> <p>If user access is not reviewed by management on a regular basis, there is a risk that access granted to users might become inappropriate with respect to the users' job roles and responsibilities over time.</p>	<p>It is our experience that access privileges tend to accumulate over time. As such, there is a need for management to perform periodic, formal reviews of the user accounts and permissions within Northgate Rev & Bens and Active Directory. These reviews should take place at a pre-defined, risk-based frequency (annually at a minimum) and should create an audit trail such that a third-party could determine when the reviews were performed, who was involved, and what access changed as a result.</p> <p>These reviews should evaluate both the necessity of existing user ID's as well as the appropriateness of user-to-group assignments (with due consideration being given to adequate segregation of duties).</p> <p>Management response:</p> <p>A review of user permissions for the Northgate Revenues and Benefits application was completed in the period from 1st April 2014 to 30th September 2014. The reviews will be completed annually between 1st July and 30th September at a minimum. Discussions are currently being held with internal audit's representatives to agree a suitable audit trail to demonstrate that this activity is completed each year.</p> <p>In addition to this HR provide a monthly report of new and departed staff. Again, this process is being reviewed to ensure that suitable audit trails are in place to trace this activity.</p> <p>ICT has also developed a process that collects leavers information from the HR systems which is then analysed by ICT staff who disable the active directory account for those people and forward the information to Money Home Job to advise them of the leaver. Again, this process is being reviewed to ensure that suitable audit trails are in place to trace this activity.</p>

Responsible officer: David Stephens – Support Manager MHJ

Appendix 1

	Assessment	Issue and risk	Recommendation
8	●	<p>Removing of leavers' access rights within Active Directory</p> <p>Security administrators within Active Directory rely on the end-user community to notify them by email of which accounts should be disabled as a result of HR activity. Because of the inconsistency associated with notifications from various members of the business, this practice leaves the potential for accounts belonging to terminated employees to remain enabled within these systems. Additionally, these administrators receive historical leaver activity to identify and remove leavers' access rights. Because of the time elapsing between termination dates and the dates these reports are provided to security administrators, this practice leaves a potential window for leavers' user accounts to remain enabled. We acknowledge that once a week one person from the support desk team checks the ending dates from iTrent and cleans the AD account, however this is not a formal process, and it is not perform by all the members of the team.</p> <p><u>This condition presents the following risk to the organisation</u> Without processes to automatically inform IT personnel of terminated users, there is a risk that the access rights of leavers are not be removed from the system, exposing the data to unauthorised access which would not be detected in a timely manner.</p>	<p>All logical access within Active Directory belonging to terminated personnel (i.e. "leavers") should be revoked in a timely manner (preferably at time of termination). The end-user community should never be solely relied upon to inform security administrators of the need to revoke logical access due to leaver activity, as such notifications are typically inconsistently provided (if at all).</p> <p>Also, while reports of historical (e.g. monthly) leaver activity enable security administrators to identify and revoke logical access associated with leavers, relying solely on such reports does not enable leavers' logical access rights to be removed in a timely manner. Instead, Active Directory administrators should be provided with: (a) timely, proactive notifications from HR of leaver activity for anticipated terminations and (b) timely, per-occurrence notifications for unanticipated terminations. Security administrators should then use these notifications to either (a) end-date user accounts associated with anticipated leavers or (b) immediately disable user accounts associated with unanticipated leavers.</p> <p>Management response: ICT have developed a solution which collects leaver information from HR systems and presents it via a front end to an ICT Support Team who then select leavers and their account in AD gets disabled. This has been tested and will be used by the whole team by the end of May 2015.</p> <p><i>Responsible Officer : Angela Birch, ICT Customer Services and Quality Manager.</i></p>

Appendix 1

	Assessment	Issue and risk	Recommendation
9	●	<p>Northgate logical access controls Passwords for the Northgate housing system are not required to consist of a mixture of letters and numbers.</p> <p>This condition presents the following risk to the organisation Passwords are compromised through guessing or brute-force attacks.</p>	<p>In addition, further development is on-going to automatically send an email to the leaver's manager informing them that the leavers account is going to be disabled. This system will allow the manager to accept or reject that action.</p> <p>Contract staff are not currently on the HR system and it is often these that start and leave in an unanticipated way. The expected end date of a contract is added to AD when the user is first set up and the process described above will also pick up these staff. Other automated emails will go to line managers as the expected end date approaches and the line manager will have the option of extending the end date.</p> <p>This additional development is expected to be completed by the end of June 2015.</p> <p><i>Responsible Officer: Angela Birch, ICT Customer Services and Quality Manager</i></p> <p>Password complexity requirements should be enabled within the Northgate application.</p> <p>Management Response:</p> <p>In terms of the Northgate system the team use for housing (not revs and benefits) – called MVM (also known as M3) only staff who have a password (which are in the main numeric and alphabetical) can access the software. Obtaining a password is limited to staff within the service</p> <p>The software needs to be on the persons individual IT account and in addition can only be accessed via the council's own server which requires the individual to already have alpha numeric log-in details anyway. Our data on MVM can't be accessed external to the council server or without the person having this alpha-numeric password</p> <p><i>Responsible officer: David Lockwood, Housing Standards and Improvement Manager</i></p>



© 2015 Grant Thornton UK LLP. All rights reserved.

'Grant Thornton' means Grant Thornton UK LLP, a limited liability partnership.

Grant Thornton is a member firm of Grant Thornton International Ltd (Grant Thornton International). References to 'Grant Thornton' are to the brand under which the Grant Thornton member firms operate and refer to one or more member firms, as the context requires. Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered independently by member firms, which are not responsible for the services or activities of one another. Grant Thornton International does not provide services to clients.

grant-thornton.co.uk