Public Document Pack

Audit, Risk & Assurance Committee

Date: Friday 21 September 2018

Time: 10.00 am **Public meeting** Yes

Venue: Room 103, West Midlands Combined Authority, 16 Summer Lane, Birmingham, B19 3SD

Membership

David Lane (Chair)	
Councillor Sucha Bains	Coventry City Council
Councillor Tom Baker-Price	Worcestershire Non-Constituent Authorities
Councillor Kerrie Carmichael	Sandwell Metropolitan Borough Council
Councillor Steve Clark	Dudley Metropolitan Borough Council
Councillor Craig Collingswood	City of Wolverhampton Council
Councillor Stephen Craddock	Walsall Metropolitan Borough Council
Sean Farnell	Coventry & Warwickshire LEP
Councillor Michael Gough	Solihull Metropolitan Borough Council
Councillor John Kraujalis	Staffordshire Non-Constituent Authorities
Councillor John O'Shea	Birmingham City Council
Councillor Alexander Phillips	Shropshire Council
Councillor June Tandy	Nuneaton & Bedworth Borough Council

Quorum for this meeting shall be nine members.

If you have any queries about this meeting, please contact:

Contact Dan Essex, Governance Services Manager
Telephone 0121 214 7505
Email Dan.Essex@wmca.org.uk

AGENDA

No.	Item	Presenting	Pages	Time
Meeting Business Items				
1.	Appointment of Vice-Chair for 2018/19	Chair	None	10:00
2.	Apologies for Absence	Chair	None	
3.	Declarations of Interest Members are reminded of the need to declare any disclosable pecuniary interests they have in an item being discussed during the course of the meeting. In addition, the receipt of any gift or hospitality should be declared where the value of it was thought to have exceeded £25 (gifts) or £40 (hospitality).	Chair	None	
4.	Chair's Remarks	Chair	None	10:05
5.	Minutes of the meeting held on 21 June 2018	Chair	1 - 6	10:10
6.	Matters Arising (a) Whistleblowing (b) Update on the latest Governance Arrangements for Fire and Police (c) Update on approach made to the Ministry of Housing Communities & Local Government regarding quorum	Chair	Verbal Report	
7.	Forward Plan	Chair	7 - 10	10:25
Business Items for Noting/Approval				
8.	External Audit of West Midlands Rail Ltd - Briefing Note	Linda Horne	11 - 12	10:30
9.	Annual Audit Letter - Year Ending 31 March 2018	Grant Patterson	13 - 24	10:40
10.	General Data Protection Regulation (GDPR) Update	Gurmit Sangha	25 - 40	10:55
11.	Internal Audit Update	Peter Farrow	41 - 46	11:05
12.	Self Assessment Exercise	Peter Farrow	47 - 66	11:20
Date of Next Meeting				
13.	Monday 12 November 2018 at 10.00am	Chair	None	

This page is intentionally left blank

WEST MIDLANDS COMBINED AUTHORITY

Audit, Risk & Assurance Committee

Thursday 21 June 2018 at 10.00 am

Minutes

Present

David Lane (Chair)	
Councillor Craig Collingswood (Vice-Chair)	City of Wolverhampton Council
Councillor Kerrie Carmichael	Sandwell Metropolitan Borough Council
Councillor Alexander Phillips	Shropshire Council
Councillor Ian Robertson	Walsall Metropolitan Borough Council
Councillor June Tandy	Nuneaton & Bedworth Borough Council
Sarah Windrum	Coventry & Warwickshire LEP

In Attendance

Councillor Joe Roberts	Dudley Metropolitan Borough Council
Councillor Jackie Taylor	Sandwell Metropolitan Borough Council

Item No. **Title**

75. Inquorate Meeting

Please note that in accordance to the WMCA Constitution, this meeting was inquorate. However, the recommendations contained within the minutes were submitted to the WMCA Board on 20 July 2018 for formal approval and adoption.

76. Apologies for Absence

Apologies for absence were received from Councillor Keith Chambers (Walsall Metropolitan Borough Council), Councillor Steve Clark (Dudley Metropolitan Borough Council), Sean Farnell (Coventry & Warwickshire LEP), John Fisher (Redditch Borough Council).

77. Declaration of Interest

Councillor Alexander Phillips declared a personal interest in minute no. 84 in respect of his membership of the Shropshire Fire & Rescue Authority.

78. Minutes of the meeting held on 16 March 2018

The minutes of the meeting held on 16 March 2018 were agreed and signed by the Chair as a correct record.

79. Matters Arising

(a) Data Security Arrangements 2017-18

The Director of Finance confirmed that all relevant information security

documentation was now ratified and published on the West Midlands Combined Authority's Sharepoint Intranet Policies and Procedures page specifically Information Security Policy, Information Classification Policy, Information Security Acceptable Use Policy and Security Operating Procedure, Mobile Device Security Operating Procedure, Internet and Email Use Policy, Information Risk Management Policy and Information Risk Management Procedure.

80. Forward Plan

The committee considered the plan of items to be reported to future meetings of the committee.

With regard to Wolverhampton Interchange Project, the Chair requested that the committee received the recommendations of the Investment Board together with the findings from the City of Wolverhampton Council at its next meeting.

The Chair asked the Director of Finance to extend an invitation to the Mayor to attend a question and answer session with Audit, Risk & Assurance Committee. The Director of Finance agreed to take this forward.

Resolved

(1) That the report be noted.

81. Strategic Risk Register

The committee considered a report of the Director of Finance that supported the committee with its responsibility of providing oversight of risk management within the West Midlands Combined Authority.

Councillor Craig Collingswood enquired about resources and the number of outstanding vacancies within the West Midlands Combined Authority. The Director of Finance clarified the number of vacancies within the organisation and assured the committee that the Authority's Leadership Team monitored the number of vacancies on a regular basis and its impact on the outputs of the organisation. The WMCA's HR Team had a plan to manage key recruitment requirements to meet 2018/19 expectations.

In addition to monitoring and addressing the risk of growth, Councillor Alexander Phillips added that the WMCA also needed to consider the risk of a recession to enable it to be in a good place to address the issues that may arise.

It was considered that the Strategic Risk Register should be presented to the next meeting of the committee for further review. Members of the committee considered that the Strategic Risk Register had become too high level and hoped that the risks and mitigation's were more granular when presented to them in September 2018.

Resolved

(1) That the content of the strategic risk register be noted.

(2) That the risk register be presented to the next meeting of the committee for further review.

82. WMCA Constitution Review Update

The committee received an update of the Head of Governance on the review of the WMCA Constitution.

The Head of Governance indicated that a draft version of the revised constitution would be available in the autumn and would be presented to the WMCA Board for adoption. The Chair asked for any changes relating to governance be presented to Audit, Risk & Assurance.

The Chair agreed to send a formal letter to the Head of Governance regarding the secondary legislation that required the Audit, Risk & Assurance Committee to have two thirds attendance of its nominated membership to be quorate. The letter was to be used by the Head of Governance in his discussions with the Ministry of Housing Communities & Local Government.

It was noted that member's attendance information was available via the WMCA's website.

Resolved

(1) That the update be noted.

83. Review of Arrangements for Standards and Conduct in the Combined Authority

The committee considered a report of the Clerk and Monitoring Officer on the review of the arrangements that had been put in place at the inception of the Combined Authority to discharge the responsibilities for standards and conduct.

The Localism Act required the appointment of an Independent Person to be consulted in the case of a complaint being considered both by the Authority and by the subject Member in the complaint. The Independent Person would assist and offer advice. The Monitoring Officer proposed that the selection of an Independent Person be made in consultation with the Chair and Vice-Chair of the committee.

There were also individuals working within the WMCA who were not covered by the Code of Conduct for elected members and therefore it was proposed that a document was to be produced that reflected the basic Code of Conduct, in which these individuals would have to sign up to. Councillor Craig Collingswood enquired about these appointments and how they were appointed on to boards. The Head of Governance agreed to provide an update at the next meeting.

Resolved

(1) That the information within the report be noted.

(2) That the Monitoring Officer be authorised to make arrangements for the selection of an Independent Person(s) in consultation with the Chair and Vice-Chair of the committee.

(3) That the Monitoring Officer finalise the arrangements for a Code of Conduct to cover individuals working within and contributing to the WMCA governance structures who were not covered by the Code of Conduct for Elected Members.

(4) That an update on the actions agreed be provided at the next meeting of the committee.

84. Devolution Deal - Update on Changes to Fire Service Governance

The committee considered a report that provided an update on the changes to the governance model for the fire service.

The Head of Governance provided further information concerning the TUPE transfer arrangements and discussions that had been held regarding the significant changes that were currently taking place within the fire service.

With regard to the funding for the West Midlands Fire & Rescue Authority, the Chair highlighted that if there were any changes to this the Audit, Risk & Assurance Committee needed to receive an update during the process to ensure that there was no risk involved. The Director of Finance proposed that this be reflected within the risk register.

The Monitoring Officer agreed to meet with the Chair during September to discuss how the Audit function for the West Midlands Fire & Rescue Authority should be absorbed by the Audit, Risk & Assurance Committee post April 2019.

[Councillor Alexander Phillips declared a personal interest in this item as he was a member of Shropshire Fire & Rescue Authority]

Resolved

(1) That the updated be noted.

85. Internal Audit Update

The committee considered a report of the Chief Audit Executive that provided an update on the work completed by the internal audit so far this financial year.

Resolved

(1) That the contents of the latest internal Audit Update report be noted.

86. Investment Portfolio Governance Audit Update 2018

The committee considered a report of the Director of Finance on the progress being made against the original recommendations in the Internal Audit review of Investment Portfolio Governance Arrangements for Programme Approval & Appraisal.

The Director of Finance provided an update on the work undertaken by Arcadis and the developments to date. The Chair proposed that a further conversation was to be had with himself and the Vice-Chair concerning the process and governance changes.

Resolved

(1) That the progress made to date against the original actions in the Internal Audit findings, detailed in the report, be noted.

(2) That the timescales for completion of recommendations from Arcadis review within section 3 of the report be noted.

(3) That the detailed review of Investment Portfolio governance and control processes undertaken by Arcadis be noted.

87. Annual Accounts 2017/18 for West Midlands Combined Authority

The committee considered a report of the S151 Officer to the Combined Authority on the Annual Accounts of the West Midlands Combined Authority and the West Midlands Integrated Transport Authority Pension Fund for the financial year ended 31 March 2018.

In addition to the WMCA Annual Accounts and Pension Fund Accounts, the committee also received a summary of the Audit Findings, the Audit Findings for both the WMCA and the Integrated Transport Authority Pension Fund and letter of representations.

The Director of Finance thanked Grant Thornton and colleagues within the WMCA Finance Team on the work undertaken on the accounts in such a short period of time and noted that the speed and quality of the accounts was excellent. The Head of Finance added that the Authority would continue to work within these timescales in the future and explained that a lessons learnt exercise would be undertaken to improve the process going forward.

It be recommended to the WMCA Board that:

(1) The Director of Finance sign the letter of representation for WMCA and the West Midlands Integrated Transport Authority Pension Fund.

(2) The annual accounts of the WMCA and the West Midlands Integrated Transport Authority Pension Fund be approved.

(3) The Audit Findings report presented by Grant Thornton be noted.

(4) Grant Thornton propose to issue an unqualified audit opinion on these accounts be noted.

(5) Subject to there being no further issues raised by Grant Thornton, the Mayor and the Director of Finance be authorised to sign the accounts on behalf of the West Midlands Combined Authority.

88. Exclusion of the Public and Press

Resolved that in accordance with section 100A(4) of the Local Government Act 1972 the press and public be excluded from the meeting for the following item of business as it involved the likely disclosure of exempt information as specified in paragraph 5 of the Act.

89. Health & Safety Governance Structures

The committee considered a report of the Director of Integrated Network Services that provided an overview of the current Governance Structure of health and safety within the West Midlands Combined Authority in addition to the boards and committees that were responsible for the effective administration of health and safety within the organisation.

The Internal Auditor explained that an audit on health and safety was currently underway and provided further details on the different elements of the audit. The Chair sought assurances from the Internal Auditor as to whether health and safety issues were being monitored at the appropriate level within the organisation, and whether the committee could release its responsibility in this area. The Internal Auditor undertook to look into this further.

The Chair requested that the proposals on how the WMCA would absorb the health and safety agenda in respect of the fire authority to be presented to its January 2019 meeting.

Resolved

(1) That the information regarding the West Midlands Combined Authority health and safety governance structures be noted.

The meeting ended at 12.05 pm.

West Midlands Combined Authority

WMCA Audit, Risk & Assurance Committee - Forward Plan

Title of Report	Description of Purpose	Date of Meeting	Lead Officer/Member
Fire Governance	To receive an update on ARACs role within Fire Governance	12 November 2018	Tim Martin
Assurance Report Update	Corporate assurance undertaken since the last update	12 November 2018	Joti Sharma
Strategic Risk Register	To receive an update on the Strategic Risk Register	12 November 2018	Joti Sharma
WMCA Vacancies - Update	To receive an update on capability and vacancy risks	12 November 2018	Rita Rais
Brexit Report	To receive a report on Brexit and the anticipated effect on finances and devolution aims. Also on the CA process used to cover risks.	12 November 2018	Tim Martin/Linda Horne
Internal Audit Update	To provide an update on audits.	12 November 2018	Peter Farrow

Title of Report	Description of Purpose	Date of Meeting	Lead Officer/Member
Assurance Report Update	Corporate assurance undertaken since the last update	14 January 2019	Joti Sharma
Internal Audit Update	To provide an update on audits	14 January 2019	Peter Farrow
Internal Audit Plan 2019/20	To approve the Internal Audit Plan	14 January 2019	Peter Farrow
External Audit Plan	To receive the External Audit Plan	14 January 2019	Grant Patterson
Strategic Risk Register	To consider and comment on the contents of the Strategic Risk Register	15 April 2019	Loraine Quibell
Annual Internal Audit Report	To note progress on audits	15 April 2019	Peter Farrow
Outturn Report 18/19	To approve the Outturn Report	15 April 2019	Tim Martin
WMCA Annual Governance Statement	To approve the Annual Governance Statement	15 April 2019	Tim Martin
WMCA Annual Accounts	To approve the WMCA Annual Accounts	21 June 2019	Linda Horne
WMCA Audit Findings	To receive an update from external audit	21 June 2019	Grant Patterson

Title of Report	Description of Purpose	Date of Meeting	Lead Officer/Member
WMITA Pension Fund – Audit Findings	To receive an update from external audit	21 June 2019	Grant Patterson/Terry Tobin
Contingency Meeting - Accounts		15 July 2019	Linda Horne

This page is intentionally left blank

Information Note to WMCA Audit, Risk & Assurance Committee:

Re: Decision made by WMR Ltd Board at 19 June meeting to not undertake an external audit of the WMR Ltd Accounts

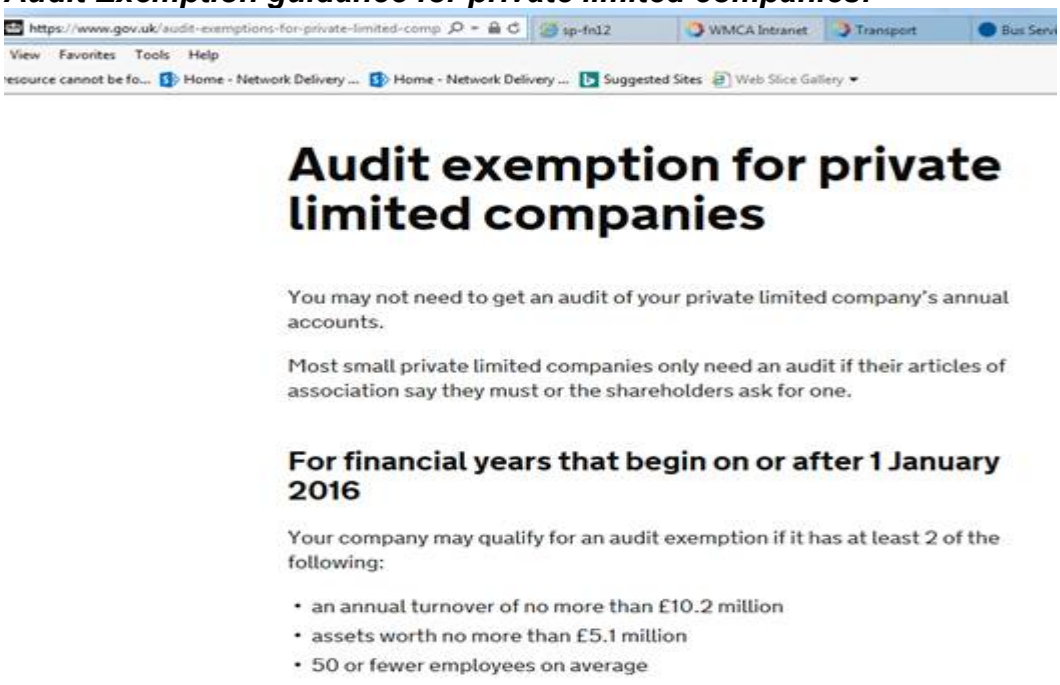
Background/Context:
At WMR Board on Tuesday 19 June 2019 it was agreed that no External Audit of the West Midlands Rail Limited accounts would be undertaken, but that this decision should be reviewed annually.

For WMCA Audit, Risk and Assurance Committee to note:
Cllr Roger Lawrence asked that the WMCA Audit, Risk & Assurance Committee is asked to note this position.

The rationale behind the WMR Board decision to not undertake an external audit of the WMR Ltd accounts is detailed below:-

- WMR Ltd comfortably meets all the audit exemption criteria for a limited company (see below)
- There is no requirement within the WMR Ltd articles of association for an auditor to be appointed
- WMR Ltd uses the systems/processes of the WMCA and these are already subject to external audit as part of the external audit of the WMCA
- Following quotes undertaken the costs of undertaking an external audit are cost prohibitive and do not represent value for money considering the size and scope of WMR Ltd.

Audit Exemption guidance for private limited companies:



Reporting of WMR Ltd Accounts:
The WMR Ltd 2017-18 accounts are scheduled to be reported to the 11 September WMR Board meeting.

WMCA Finance Team opinion of WMR Board decision:
As there was limited activity taking place during 2017-18 with WMR Limited only being financially active from the start of the new West Midlands Rail franchise in December 2017 (and dormant prior to this) then the WMCA finance team is supportive of the above rationale behind this decision but recommends that this is reviewed for next year.

Annual Audit Letter

Year ending 31 March 2018

West Midlands Combined Authority
16 August 2018

Contents

Your key Grant Thornton team members are:

Grant Patterson
Director
T: 0121 232 5296
E: grant.b.Patterson@uk.gt.com

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

Ellena Grant-Pearce
Executive
T: 0121 232 5397
E: Ellena.grant-pearce@uk.gt.com

Executive Summary

Purpose

Our Annual Audit Letter (Letter) summarises the key findings arising from the work that we have carried out at West Midlands Combined Authority (the Authority) for the year ended 31 March 2018, including the West Midlands Integrated Transport Authority Pension Fund (the Pension Fund) accounts.

This Letter is intended to provide a commentary on the results of our work to the Authority and external stakeholders, and to highlight issues that we wish to draw to the attention of the public. In preparing this Letter, we have followed the National Audit Office (NAO)'s Code of Audit Practice and Auditor Guidance Note (AGN) 07 – 'Auditor Reporting'. We reported the detailed findings from our audit work to the Authority's Audit, Risk & Assurance Committee as those charged with governance in our Audit Findings Reports on 21 June 2018 with formal approval by the Authority's Board on 20 July 2018.

Respective responsibilities

We have carried out our audit in accordance with the NAO's Code of Audit Practice, which reflects the requirements of the Local Audit and Accountability Act 2014 (the Act). Our key responsibilities are to:

- give an opinion on the Authority's and Pension Fund's financial statements (section two)
- assess the Authority's arrangements for securing economy, efficiency and effectiveness in its use of resources (the value for money conclusion) (section three).

In our audit of the Authority's financial statements (which include the Pension Fund), we comply with International Standards on Auditing (UK) (ISAs) and other guidance issued by the NAO.

Our work

Materiality	We determined materiality for the audit of the Authority's financial statements to be £4.643m, which is 1.8% of the Authority's gross revenue expenditure. We determined materiality for the audit of the Pension Fund accounts administered by the Authority to be £4.92m, which is 1% of the Pension Fund's net assets.
Financial Statements opinion	We gave an unqualified opinion on the Authority's financial statements on 20 July 2018. We gave an unqualified opinion on the Pension Fund accounts of the West Midlands ITA Pension Fund on 20 July 2018.
Whole of Government Accounts (WGA)	We completed work on the Authority's consolidation return following guidance issued by the NAO.
Use of statutory powers	We did not identify any matters which required us to exercise our additional statutory powers.
Value for Money arrangements	We were satisfied that the Authority put in place proper arrangements to ensure economy, efficiency and effectiveness in its use of resources. We reflected this in our audit report to the Authority on 20 July 2018.
Certificate	We are not able to certify the conclusion of the audit as we are required to give an opinion on the consistency of the Pension Fund financial statements of the Authority included in the Pension Fund Annual Report with the pension fund financial statements included in the Statement of Accounts. The Pension Fund Annual Report is not required to be published until 1 December 2018 and was not available at the time of our audit or this letter. We are therefore yet to issue our report on the consistency of the Pension Fund financial statements. Until we have done so, we are unable to certify that we have completed the audit of the financial statements.

Audit of the Accounts

Our audit approach

Working with the authority

We have delivered a number of successful outcomes working alongside you:

- **An efficient audit** – we delivered an efficient audit with you in May and June, delivering the accounts 28 working days before the deadline, releasing your finance team for other work.
- **Sharing our insight** – we provided regular audit committee updates covering best practice. We also shared our thought leadership reports
- **Providing training** – we provided your teams with training on financial accounts **Supporting development** – we provided training for the Audit, Risk & Assurance Committee on 19 January 2018.

We would like to record our appreciation for the assistance and co-operation provided to us during our audit by the Authority's staff.

Materiality

In our audit of the Authority's financial statements (including the Pension Fund), we use the concept of materiality to determine the nature, timing and extent of our work, and in evaluating the results of our work. We define materiality as the size of the misstatement in the financial statements that would lead a reasonably knowledgeable person to change or influence their economic decisions.

Authority Materiality

We determined materiality for the audit of the Authority's accounts to be £4.643m, which is 1.8**%** of the Authority's gross revenue expenditure. We used this benchmark as, in our view, users of Authority's financial statements are most interested in where the Authority has spent its revenue in the year.

We set a lower threshold of £100,000, above which any errors we identified in respect of senior officers remuneration would be reported to the Audit, Risk & Assurance Committee in our Audit Findings Report.

We also set a lower level of specific materiality of £100,000 for senior officer remuneration as we considered these disclosures to be sensitive and of specific interest to the reader of the accounts.

Pension Fund Materiality

For the audit of the West Midlands ITA Pension Fund accounts, we determined materiality to be £4.92m, which is 1% of the Fund's net assets. We used this benchmark as, in our view, users of the Pension Fund accounts are most interested in the value of assets available to fund pension benefits.

We considered the need to set lower levels of materiality for sensitive balances, transactions or disclosure in the accounts, and determined not to set any lower levels.

The scope of our audit

Our audit involves obtaining sufficient evidence about the amounts and disclosures in the financial statements to give reasonable assurance that they are free from material misstatement, whether caused by fraud or error. This includes assessing whether:

- the accounting policies are appropriate, have been consistently applied and adequately disclosed;
- the significant accounting estimates made by management are reasonable; and
- the overall presentation of the financial statements gives a true and fair view.

We also read the remainder of the Statement of Accounts and the narrative report, and annual governance statement published alongside the Statement of Accounts to check they are consistent with our understanding of the Authority and with the financial statements included in the Statement of Accounts on which we gave our opinion.

We carry out our audit in accordance with ISAs (UK) and the NAO Code of Audit Practice. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Our audit approach is based on a thorough understanding of the Authority's business and is risk based.

We identified key risks and set out overleaf the work we performed in response to these risks and the results of this work.

Audit of the Accounts

Authority Significant Audit Risks

These are the significant risks which had the greatest impact on our overall strategy and where we focused more of our work.

Risks identified in our audit plan	How we responded to the risk	Findings and conclusions
Improper revenue recognition Under ISA 240 there is a presumed risk that revenue may be misstated due to the improper recognition of revenue. This presumption can be rebutted if the auditor concludes that there is no risk of material misstatement due to fraud relating to revenue recognition.	Having considered the risk factors set out in ISA 240 and the nature of the revenue streams at the Authority, we determined that the risk of fraud arising from revenue recognition could be rebutted, because: • 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 West Midlands Combined Authority, mean that all forms of fraud are seen as unacceptable	Based on the rebuttable we did not consider this to be a significant risk for West Midlands Combined Authority and we identified no issues in respect of revenue recognition in the course of our work.
Management override of internal controls Under ISA 240 there is a non-rebuttable presumed risk that the risk of management over-ride of controls is present in all entities. The Authority faces external scrutiny of its spending, and this could potentially place management under undue pressure in terms of how they report performance. We identified management override of controls as a risk requiring special audit consideration.	As part of our audit work we: • documented an understanding of the accounting estimates, judgements applied and decisions made by management and • considered their reasonableness • obtained a full listing of journal entries, identify and tested unusual journal entries for appropriateness • evaluated the rationale for any changes in accounting policies or significant unusual transactions.	Our audit work has not identified any issues in respect of management override of controls.

Audit of the Accounts

Authority Significant Audit Risks (continued)

These are the significant risks which had the greatest impact on our overall strategy and where we focused more of our work.

Risks identified in our audit plan	How we responded to the risk	Findings and conclusions
Valuation of the Authority's pension fund net liability The Authority's pension fund asset and liability as reflected in its balance sheet represent a significant estimate in the financial statements. We identified the valuation of the pension fund net liability as a risk requiring special audit consideration.	As part of our audit work we: • reviewed the pensions prepayment paid by the Authority to the West Midlands Pension Fund in April 2017 • identified the controls put in place by management to ensure that the pension fund liability is not materially misstated and also assessed whether these controls were implemented as expected and whether they were sufficient to mitigate the risk of material misstatement • evaluated the competence, expertise and objectivity of the actuary who carried out your pension fund valuation and gained an understanding of the basis on which the valuation is carried out • undertook procedures to confirm the reasonableness of the actuarial assumptions made • checked the consistency of the pension fund asset and liability and disclosures in the notes to the financial statements with the actuarial report from your actuary.	Through our review of the pensions prepayment we were satisfied it was subject to due process and has been accounted for in the financial statements correctly. PwC were engaged by the Audit Commission (and subsequently the NAO) as consulting actuary to undertake a central review of the actuaries used by the Local Government Pension Scheme (LGPS). PwC produced a report designed to provide support to auditors when assessing the competence and objectivity of, and assumptions and approach adopted by, actuaries producing IAS 19 figures in respect of the LGPS, Police and Fire schemes as at 31 March 2018. We used this report to inform our assessment of the valuation of the pension fund liability in the Authority's accounts. The liability as at 31 March 2017 was £57.166m. This has reduced during the year by £6.953m to £50.213m. We compared the assumptions used by the Authority's actuary against industry benchmarks and based on the work performed we are able to conclude that management's assumptions overall are reasonable. The value of the net pension liability in the balance sheet is not equal to the pension reserve of £55.377m. We are satisfied that this is appropriate, as the difference is due to the prepayment of £5.164m referred to above. Our audit work has therefore not identified any issues in respect of the pension fund net liability.

Audit of the Accounts

Pension Fund Significant Audit Risks

These are the risks which had the greatest impact on our overall strategy and where we focused more of our work on the pension fund.

Risks identified in our audit plan	How we responded to the risk	Findings and conclusions
Improper revenue recognition Under ISA 240 there is a presumed risk that revenue may be misstated due to the improper recognition of revenue. This presumption can be rebutted if the auditor concludes that there is no risk of material misstatement due to fraud relating to revenue recognition.	Having considered the risk factors set out in ISA 240 and the nature of the revenue streams at the Authority, we determined that the risk of fraud arising from revenue recognition could be rebutted, because: • 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 West Midlands Combined Authority as the administering body, mean that all forms of fraud are seen as unacceptable	Based on the rebuttable we did not consider this to be a significant risk for West Midlands ITA Pension Fund and we identified no issues in respect of revenue recognition in the course of our work.
Management override of internal controls Under ISA 240 there is a non-rebuttable presumed risk that the risk of management over-ride of controls is present in all entities. The Pension Fund faces external scrutiny of its spending, and this could potentially place management under undue pressure in terms of how they report performance. We identified management override of controls as a risk requiring special audit consideration.	As part of our audit work we: • documented an understanding of the accounting estimates, judgements applied and decisions made by management and considered their reasonableness • obtained a full listing of journal entries, identify and tested unusual journal entries for appropriateness • evaluated the rationale for any changes in accounting policies or significant unusual transactions.	Our audit work has not identified any issues in respect of management override of controls.
Valuation of level 3 investments Under ISA 315 significant risks often relate to significant non-routine transactions and judgemental matters. Level 3 investments by their very nature require a significant degree of judgement to reach an appropriate valuation at year end. We identified the valuation of level 3 investments as a risk requiring special audit consideration.	As part of our audit work we have: • gained an understanding of the Fund's process for valuing level 3 investments and evaluated the design of the associated controls • reviewed the qualifications of the expert, Barnett Waddingham, to value Level 3 investments at year end • reviewed the nature and basis of estimated values and consider what assurance management has over the year end valuations provided by these types of investments. We used our in-house experts, the Grant Thornton valuation team, to assist us in doing this. We reviewed the assumptions and calculations to provide assurance that the Pension Fund's valuation model was reasonable.	We independently estimated the value of the insurance buy-in to be £238,296,000 compared to the Pension Fund's actuarial valuation of £238,333,000. The valuation of this estimate is complex and is within 0.02% of the actuary's result and within our expected range. From this we have concluded that the valuation is reasonable and not materially misstated.

Audit of the Accounts

Audit opinion

We gave unqualified opinions on both the Authority's financial statements and the pension fund accounts of West Midlands ITA Pension Fund on 20 July 2018, in advance of the national deadline.

Preparation of the accounts

The Authority and Pension Fund presented us with draft accounts in accordance with the national deadline, and provided a good set of working papers to support them. The finance team responded promptly and efficiently to our queries during the course of the audits.

Issues arising from the audit of the accounts

We reported the detailed findings from our audit work to the Authority's Audit, Risk & Assurance Committee as those charged with governance in our Audit Findings Reports on 21 June 2018.

Due to quoracy issues formal authorisation and approval to publish the financial statements (before which we cannot issue our opinion and which had been delegated to the Committee) had to be deferred to the WMCA Board at its meeting on 20 July 2018. The Authority is seeking to amend the Establishment Order in order to modernise the quoracy requirements to reduce the risk of this occurring again.

Annual Governance Statement and Narrative Report

We are required to review the Authority's Annual Governance Statement and Narrative Report. It published them on its in the Statement of Accounts in line with the national deadlines.

Both documents were prepared in line with the CIPFA Code and relevant supporting guidance. We confirmed that both documents were consistent with the financial statements prepared by the Authority and with our knowledge of the Authority.

Certificate of closure of the audit

We are also required to certify that we have completed the audit of the accounts of the West Midlands Combined Authority in accordance with the requirements of the Code of Audit Practice.

We are not able to certify the conclusion of the audit at this time as we are required to give an opinion on the consistency of the Pension Fund financial statements of the Authority included in the Pension Fund Annual Report with the pension fund financial statements included in the Statement of Accounts. The Pension Fund Annual Report is not required to be published until 1 December 2018 and was not available at the time of our audit or this letter. We are therefore yet to issue our report on the consistency of the Pension Fund financial statements. Until we have done so, we are unable to certify that we have completed the audit of the financial statements.

Value for Money conclusion

Background and key findings

We carried out our review in accordance with the NAO Code of Audit Practice, following the guidance issued by the NAO in November 2017 which specified the criterion for auditors to evaluate: *In all significant respects, the audited body takes properly informed decisions and deploys resources to achieve planned and sustainable outcomes for taxpayers and local people.* Our first step in carrying out our work was to perform a risk assessment and identify the key risks where we concentrated our work. The key risks we identified and the work we performed are set out below.

Risks identified in our audit plan and how we responded to the risk	Findings
Evolution of the governance arrangements As noted in our prior year Audit Findings Report, the governance arrangements at the Authority are continuing to develop as the Authority itself evolves. Since last year the Authority has appointed its substantive senior management team which will pave the way for further evolution of governance arrangements. A second devolution deal to promote growth was announced in November 2017 and there are on-going discussions in respect of responsibilities for fire and rescue services in the region. There is a risk that arrangements may not appropriately reflect the changing responsibilities of the Authority and heighten the risk of actual or perceived instances of inadequate governance. **Our response** As part of our work we have reviewed relevant Board and Combined Authority papers and held discussions with management and key officers about any changes to the governance structure as well as to understand how decisions are made and reported to the Board.	During the 2016/17 financial year the Authority made a number of changes to its governance structure to as it has developed from the Centro group. Key elements included: • revising the Constitution including the Scheme of Delegation • setting up a Committee to oversee audit, risk and assurance • establishing a new Assurance Framework • developing a Risk Management Strategy and risk register Since then the Authority has continued to evolve and is starting to embed the above elements. Risk discussions have been formalised with directors on an ongoing basis. The Strategic Risk Register is developing further and is reviewed on a quarterly basis at Senior Leadership Team meetings. The ownership of the risk register is more established than as at 31 March 2017, at which time the senior leadership team, including the Mayor, were not yet in place. That they have been in a position as a team now, for approximately 5 months as at 31 March 2018, is reflected in the achievements noted in the Review of the Year section of the Narrative Report. We are cognisant of the fact that the Authority is, at times, beholden to activities, requests and demands upon it that are outside of its control. Therefore it behoves the Authority to be as nimble and agile as possible in order to respond to these demands, and, where possible to be proactive as much as reactive. We note from our review of the Narrative Report within the financial statements at Table 1 that as at February 2018 there were 105.5 vacancies being carried. Left unresolved, this is a risk to the Authority's ability to continue to manage and absorb the increased levels of activity that are expected, especially with the ever widening remit of the Combined Authority expected over the coming 12 to 24 months. For example the Authority will see the West Midlands Fire and Rescue Services come within its governance structure as well as the transfer of the adult skills funding, which brings with it a budget of £112 million per annum. The Authority acknowledge this risk and are tracking vacancies as part of its recruitment drive. The latest tracker provided to us shows that approximately a third of the vacancies are currently appointed or being recruited to, with plans in place to fill the remainder across the course of the year. The Authority recognise that it doesn't necessarily have to do everything itself but can convene and blend where appropriate. As an example, it has commissioned Arcadis to carry out a controls and assurance review of the Investment Programme with a view to maximising delivery of benefits and outcomes, by recommending improvements to the Investment Programme governance. Arcadis has also undertaken an audit on the corporate risk management process, provided commentary and recommendations across the key themes of: Risk Strategy & Governance, Risk Management Process, Culture & People and Systems & Tools. Lessons learned from these reviews can then be applied to other areas, as with appropriate governance arrangements in place, alongside capacity, resourcing and capability sufficiency, the Authority will be able to mobilise quickly, whilst still being clear on purpose.

Overall Value for Money conclusion

On the basis of the work performed we have concluded that the risk was sufficiently mitigated and we are therefore satisfied that the Authority put in place proper arrangements for securing economy, efficiency and effectiveness in its use of resources for the year ended 31 March 2018.

A. Reports issued and fees

We confirm below our final reports issued and fees charged for the audit and the following non-audit service was identified:

Reports issued

Report	Date issued
Audit Plan	19 January 2018
Audit Findings Report	21 June 2018
Annual Audit Letter	August 2018

Fees

	Planned £	Actual fees £	2016/17 fees £
Statutory Authority audit	46,500	46,500	46,500
Audit of Pension Fund	21,000	21,000	21,000
Total fees	**67,500**	**67,500**	**67,500**

The planned fees for the year were in line with the scale fee set by Public Sector Audit Appointments Ltd (PSAA).

Fees for non-audit services

Service	Fees £
Audit related services - None	Nil
Non-Audit related services - Strategic Financial Management Development Programme: attendance of 1 delegate from the Authority	£2,750

Non- audit services

- For the purposes of our audit we have made enquiries of all Grant Thornton UK LLP teams providing services to the Authority. The table above summarises all non-audit services which were identified.
- We have considered whether non-audit services might be perceived as a threat to our independence as the Authority's auditor and have ensured that appropriate safeguards are put in place.

The above non-audit services are consistent with the Authority's policy on the allotment of non-audit work to your auditor.

This page is intentionally left blank

Audit, Risk & Assurance Committee

Date	21 September 2018
Report title	General Data Protection Regulation (GDPR) Update
Accountable Chief Executive	Deborah Cadman, West Midlands Combined Authority email: deborah.cadman@wmca.org.uk tel: (0121) 214 7200
Accountable Employee	Gurmit Sangha , Data Protection & Information Sharing Officer email: gurmit.sangha@wmca.org.uk tel: (0121) 214 7301
Report has been considered by	

Recommendation(s) for action or decision:

The WMCA Audit, Risk & Assurance Committee is recommended to

(1) Consider and comment on this report.

1.0 Purpose

On 25 May 2018 the Data Protection Act 2018 came into force, introducing the General Data Protection Regulation (GDPR) into UK law. The purpose of this report is to provide an update on West Midlands Combined Authority (WMCA) meeting its responsibilities and compliance with the new legislation.

2.0 Background

Since September 2017 significant progress has been made by building on WMCA's commitment to the pre GDPR regime, and ensuring that the core elements of GDPR have been met and plans are in place to address ongoing requirements.

This report is intended to update the Committee on the work undertaken prior to GDPR going live, the approach going forward, and the work on addressing the recommendations from two reports commissioned by WMCA on GDPR.

3.0 Activity leading up to GDPR go live on 25 May 2018

The focus in the months before 25 May was to address the areas where WMCA processes personal data on a daylily basis as part of its operations. Some of the main areas of work were:

- All departments engaging with the Data Protection Officer (DPO) to establish the work required in their area to meet the new standard.
- All departments creating Information Asset Registers mapping out the data they hold, and how it flows through the WMCA.
- The DPO reviewed WMCA lawful grounds for processing data in light of the forthcoming changes to the law. Where required these were amended and the way in which data is collected, used or held changed.
- Data protection policies, procedures, and guidance were updated.
- Key data protection roles were introduced including a Senior Information Risk Owner (SIRO), and Information Asset Owners (IAO) for each department. Their responsibilities have been defined within the WMCA Information Assurance Framework and training provided to them.
- All Privacy Notices were redrafted to reflect the forthcoming legislation.
- Where required data subjects were contacted to explain the forthcoming changes.
- Standard WMCA contracts were amended to include the mandatory GDPR clauses.
- The process for amending existing WMCA contracts with data processors was commenced to reflect the new mandatory GDPR clauses.
- The GDPR concept of privacy by design was introduced. A Data Privacy Impact Assessment template with supporting guidance has been drafted and published to assist in the delivery of this concept.
- The seven data subject rights introduced by GDPR were highlighted across the WMCA. The process by which we will manage any data subject exercising such a right has been made clear both internally and externally. Teams have been advised on holding data in a manner which can support WMCA compliance.
- All staff were required to complete mandatory data protection and GDPR training.

- The role of DPO has been introduced, developed and highlighted across the organisation as a central point of contact for advice on data protection matters. The introduction of this role has seen an increase in advice being sought on data protection issues both at departmental level, and in relation to specific projects and programmes. The DPO has also taken responsibility for addressing any external queries raised by members of the public on data protection matters.

During May WMCA successfully moved from the Data Protection Act 1998 regime to the new GDPR (Data Protection Act 2018) regime, with no major concern.

However we recognise that GDPR compliance is not focused on a fixed point in time. Much of what the new legislation mandates will be an ongoing process. Since May 2018 WMCA has had in place a dedicated Data Protection Officer to lead on this work. It is also important to recognise that in many areas we, like all other organisations, will improve and develop as new concepts introduced by GDPR are embedded and developed. Examples include Data Privacy Impact Assessments, Information Asset Registers, training and development to increase staff data protection awareness.

4.0 WMCA approach to GDPR Compliance post go live on 25 May 2018

The expectation of the Information Commissioner (ICO) is that any organisation subject to an investigation must be able to evidence its commitment to meeting the GDPR standard, and the activity it has undertaken to address data protection. An organisation will be required to demonstrate this both strategically, and specifically within the area where any legislative breach may have occurred. With this in mind the immediate focus is in advancing the following now established areas:

- Clear and focused governance arrangements which provide control measures to protect data. Ensuring these are not only in place but understood.
- Organisational commitment to data protection that is cross-organisational, through all levels with everyone understanding their responsibilities.
- Creating a culture of transparency and accountability as to how we use personal data, both internally and externally.
- Understanding the information we hold, where it has come from, and who we share it with.
- Implementing accountability measures by:
  - Understanding our lawful basis to process the data we hold
  - Ensuring Privacy Notices are compliant,
  - Conducting Data Protection Impact Assessments to ensure “privacy by design” and
  - Ensuring our contracts with partner organisations are compliant with the GDPR standard.
- Ensuring appropriate security by making sure we have continual rigor in identifying, and taking appropriate steps to address security vulnerabilities and cyber risks.
- Training all that work at WMCA with regular and refresher training and awareness. Recognising that staff are our best defense against a breach of the legislation, but can also potentially be the greatest weakness.

Work is underway to create a central data protection portal within the WMCA intranet which will provide a central point available to all staff on data protection issues. This will not only aid awareness but also the management of GDPR compliance. Additionally to supplement the introduction of mandatory annual data protection training a programme of regular data protection awareness alerts will be introduced by October 2018.

A programme of internal data protection audits to provide monitoring and guidance for departments will also be introduced.

5.0 Internal Audit of Data Security Arrangements & externally commissioned GDPR Gap Analysis Report

To seek assurance that effective progress is being made towards compliance an internal audit of data security arrangements was completed in March 2018. This supplemented an external gap analysis review commissioned in December 2017, from which an action plan was developed. The work leading up to GDPR, and since its introduction has been underpinned by these documents.

We are nearing a position of completing the work required by the recommendations from these reports and seeking their closure. Those recommendations which remain open are now moving into the area of ongoing business as usual work we are required to undertake by the legislation.

Appendix A below provides an update on the 4 recommendations from the Internal Audit of Data Security Arrangements.

Appendix B below provides an update on the 37 action points from the externally commissioned GDPR Gap Analysis Report.

Completion of actions and "Signing off" for closure.

The action points form the Gap Analysis Report are to be signed off for closure by the Senior Information Risk Owner. Appendix A sets out the anticipated dates for their completion.

A meeting has been arranged with the Auditor to discuss closure of all recommendations from the Internal Audit. We anticipate being in a position to submit a report to the Audit Risk & Assurance Committee by 30 September 2018 recommending completion and closure of the report.

Appendix A: Internal Audit of Data Security Arrangements recommendations update September 2018

Action is imperative to ensure that the objectives for the area under review are met — Red			
No	**Recommendation**	**Update**	**Target date for closure**
2.1	A robust and suitably detailed action plan should be established to support the implementation of the actions and tasks required to achieve GDPR readiness and to ensure that the issues identified in the external review are appropriately, explicitly and fully addressed. Explicit implementation dates (with appropriate prioritisation) should be stated in the plan against each action and include a more detailed breakdown of medium to long term timescales where applicable. Until the Information Assurance Framework is fully operational, alternative action owners should be identified for each specific GDPR related action. Once established the GDPR action plan should be periodically reviewed, progress monitored and appropriately reported to the responsible officer and /or the Senior Information Risk Owner.	The GDPR compliance work stream has been formalised into a managed project with a project outline/proposal, project initiation document, and detailed implementation and action plan. The action plan was developed in conjunction with the externally commissioned GDPR Gap Analysis Report. The plan documents the action required to meet gaps in GDPR compliance, milestones, reviews, action owners, etc **Status:** Progress to be reviewed by Internal Auditor for closure.	12 November 2018 (Subject to ARAC approval)

Action is required to avoid exposure to significant risks in achieving objectives — Amber			
No	**Recommendation**	**Update**	**Target date for closure**

Action is required to avoid exposure to significant risks in achieving objectives **Amber**			
No	**Recommendation**	**Update**	**Target date for closure**
2.2	A review should be undertaken to ensure that appropriate policies are available to employees in the interim until such time that the Information Assurance Framework has been fully implemented. All redundant policies should be archived or removed. An organisational wide awareness programme should be undertaken to cover both GDPR readiness and development of the Insurance Assurance Framework and its underlying policies and procedures. This should extend from the WMCA Board to operational levels of the WMCA. A communications plan should be developed to support implementation of GDPR readiness and the Information Assurance Framework.	An Information Assurance Framework was established in January 2018 and work continues to imbed this within the WMCA. The following policies have been updated to incorporate the new provisions and published: • Data Protection Policy • Information Assurance and Information Security Management • Information Risk Management Policy • Information Risk Management Procedure • Information Security Acceptable Use Policy and Security Operating Procedures (SyOPs) • Information Security Classification Policy • Information Security Policy • Internet and Email Use Policy • Mobile Device Security Operating Procedures (SyOPs) • Data Subject Rights Guidance for Staff The HR induction programme now includes training and awareness of the above. The content of the above polices will feed onto the annual data protection awareness programme. **Status:** Progress to be reviewed by Internal Auditor for closure.	12 November 2018 (Subject to ARAC approval)
2.3	GDPR readiness activities should be formally established as a project supported by robust, specific and appropriate governance, roles and responsibilities, project management, risk management and reporting arrangements. The wider Information Assurance Framework implementation exercise should also be established ideally as a programme	The GDPR readiness programme was undertaken by the following officers; Cyber Security Specialist, appointed WMCA Lawyer, Data Protection Officer, Departmental Information Asset Owners, and a number of appointed officers within departments. The work has been enshrined within project management principles.	12 November 2018 (Subject to ARAC approval)

Action is required to avoid exposure to significant risks in achieving objectives **Amber**			
No	**Recommendation**	**Update**	**Target date for closure**
	under which specific projects or workstreams should be established, including GDPR readiness as a discrete project. A suitably resourced multi-disciplined programme / project team should be created with appropriate representation and supported by appropriate terms of reference, governance and reporting arrangements.	There has been regular reporting to the Senior Information Risk Owner (SIRO) and WMCA Audit, Risk & Assurance Committee Going forward an Information Assurance Group made up of the Senior Information Risk Owner, Information Asset Owners, the Data Protection Officer and Cyber Security Specialist has been established. The group will lead on the WMCA ongoing information assurance programme. **Status:** Progress to be reviewed by Internal Auditor for closure	
2.4	The role of the Data Protection Officer should be explicitly included in the Information Assurance Framework with associated responsibilities. Clarity within the action plan should be evidenced to ensure that any actions that would be undertaken by a Data Protection Officer have been clearly assigned to the Solicitor in the interim until the Data Protection Officer has been appointed.	The post of Data Protection Officer (DPO) has been created and the DPO has been in post since 1 May 2018. The position is incorporated within the Information Assurance Framework. The role is being embedded within the WMCA as a point of advice and guidance for teams, project managers and departments. The DPO leads on all GDPR and data protection compliance matters. **Status:** Progress to be reviewed by Internal Auditor for closure.	12 November 2018 (Subject to ARAC approval)

Appendix B: GDPR Gap Analysis Report action plan update September 2018

Recommendation	Priority	Update	Anticipated closure date
1. Governance			
1a) The board, executive team, and senior and functional managers have differing awareness of the GDPR's requirements and their implications for the authority. Everyone in top management needs to have the same level of awareness. This could be achieved through, for example, an in-house GDPR Foundation course (with exam at discretion). Individual roles and responsibilities should be added to job descriptions.	High	WMCA Information Assurance Framework, agreed at Leadership Team level, establishes executive and senior management roles and responsibilities and provides ToRs for the Senior Information Risk Owner (SIRO) and Information Asset Owners (IAO). The Framework also includes the requirement for mandatory annual GDPR and Information Security training and awareness for all users and at all levels. The first wave of this training has been completed. The option to tailor future training to meet roles and responsibilities is being explored. An ongoing organisational wide awareness programme is being developed to provide a foundation level understanding for all.	30 November 2018
1b) The board should receive regular updates on the progress towards closing the compliance gap. This should be part of the accountable director's role. The board does currently receive regular audit reports on DPA/GDPR compliance, so this should continue to be included in any future internal audit plan and reported regularly. The GDPR should also be included as a standard item on the agenda of board meetings.	High	The Information Assurance Framework establishes strategic internal information assurance review by the WMCA Information Assurance Group, chaired by the SIRO and core attended by all Information Asset Owners, DPO and Cyber Security Specialist. All information assurance projects and identified strategic risks are reported and managed at this level.	30 September 2018
2. Risk management			
2a) Although the authority has an information security policy (based on HMG's Information Assurance Standards) there is no formal process for the management of risks to data privacy. Privacy risk is on the board-level corporate risk register, but the board and the authority need to develop their understanding of the idea of risk to the rights and freedoms of natural persons, as distinct from risk to the authority. GDPR compliance and privacy both need to be reviewed on a regular basis by the board, which	High	An Information Risk Management Policy and Procedure, inclusive of SIROs risk appetite, in support of the Information Assurance Framework, is now in place. The policy includes mechanisms for the identification and management of "Impact on the Privacy of the Citizen" risk. The review and management of this risk is a function of the relevant Information Asset Owner,	30 September 2018

needs to determine – possibly by means of a half-day workshop – an appropriate and objectively expressed information risk appetite that can drive and inform the information risk assessment process.		operationally, and the SIRO with the Information Assurance Group strategically. The DPO supports and advices on the management and mitigation of privacy risk, and will hold an Information Risk Register. Reporting to the Information Assurance Group and SIRO has been put in place. Any organisationally critical risks will feed into WMCA risk registers.	
2b) WMCA should ensure the GDPR and privacy risk are considered in all relevant risk assessments. This should be defined in a documented risk assessment methodology to ensure application across all areas of the business.	High	As at 2a (above)	30 September 2018
2c) GDPR and privacy risk should be included in any control frameworks that set out risk controls and treatment.	High	As at 2a (above)	30 September 2018
3. GDPR project			
3a) WMCA has established only two members of a GDPR project team to ensure the authority has a coordinated strategy, systematically implemented, to achieve an acceptable level of GDPR compliance in the available time. This project team will need to be expanded, must set out a clear plan for achieving GDPR compliance by 25 May 2018 and will need training, external resources and clear top management support (via the accountable director).	High	The role of an autonomous DPO has been established and filled. The project team was expanded to include the Cyber Security Specialist, WMCA lawyer, DPO, Information Asset Owners, and appointed officers within departments. The Senior Information Risk Owner (Director of Finance) is the accountable Officer.	Closed
3b) WMCA could arrange for the relevant project personnel to attend a GDPR Practitioner course (which can be delivered in-house).	Medium	The appointed DPO holds a Data Protection Practitioner qualification, and has been leading the compliance programme since May 2018.	Closed
4. DPO			
4a) WMCA is processing personal data, including limited amounts that fall into the special categories of personal data (e.g. health data). As a public body, the authority is obliged to appoint a DPO in terms of Article 37.1(a) and has appointed its in-house solicitor as DPO designate. However, care should be taken before allocating any DPO role to an existing staff member	Very high	An autonomous DPO was recruited and started work in May 2018	Closed

to take account of the provisions of Article 38 of the GDPR regarding avoiding conflicts of interest. Selection of the DPO is urgent as the role is essential for key areas of the compliance project. The DPO role is set out in the GDPR and was discussed in detail during the gap analysis.			
4b) The DPO should report to the board regularly via the nominated director for oversight of GDPR compliance. This will ensure an appropriate level of input to senior management while securing independence for the DPO role (Article 38).	High	The DPO will provide reports to the Information Assurance Group which the Senior Information Risk Owner Chairs.	Closed
5. Roles and responsibilities			
5a) WMCA should implement an authority-wide GDPR awareness programme and make GDPR training a part of staff induction. Although the functional managers interviewed appeared to have a grasp of the basics of data protection, more specific GDPR-oriented training is required for management. Completion of the awareness training should be measured and reported to the board periodically. Employees should have data protection responsibility included in their job descriptions, particularly those with specific objectives such as information asset owners.	High	Information Assurance Framework establishes mandatory Data Protection and Information Security education and awareness to all users. This will take place annually and will be supplemented by privacy awareness initiatives during the course of each year. The first annual all staff training package has been completed. Bespoke training for identified post holders is being explored. The HR induction programme has been developed to include privacy training.	30 September 2018
5b) Aside from the compliance project team core members, WMCA currently has no specific roles for planning compliance with the GDPR (e.g. 'data champions'). The roles and responsibilities for delivering GDPR compliance, and for maintaining that compliance after the implementation date next year, need to be made clear.	High	The roles and responsibilities of Information Asset Owners have been established. The advantages of data champions within teams is recognised, and we will work to develop this concept.	31 December 2018
6. Scope of compliance			
6a) WMCA must determine its status with regard to all the personal data that it processes – i.e. as a data controller or as a data processor, as well as any data-sharing activity. Interviews identified most of the processes and databases that involve or store personal data, as well as issues and risks with these processes. Action points were identified during interviews.	High	Substantial work has been undertaken in establishing WMCA legal status in the individual areas where we process data. The DPO has advised departments, teams, and project managers across the WMCA ensuring the status is clearly understood. The corresponding GDPR issues have been addressed, including the amendment of	30 September 2018

These included specific areas of risk to data processed. Cross-border processing is a feature of the scope for WMCA.		contracts, sharing agreements, relationships with partner organisations, service level agreements, customer terms and conditions.	
6b) The scope of a PCF should include all personal data processed; services and support provided by WMCA staff and contractors; and all legal entities identified by WMCA, including any associated companies that are themselves data controllers/processors (e.g. Man Commercial Protection Ltd).	High	As at 6a (above)	30 September 2018
6c) WMCA should identify all third-party organisations, partners and entities (e.g. suppliers or processors) that might process and/or share data, and ensure this sharing is documented in the register of processing required by Article 30. Such documentation should be maintained (see 8h below).	High	As at 6a/b (above)	30 September 2018
6d) WMCA should perform a review of current contracts with data processors to ensure all relevant GDPR provisions have been included (Article 28). This should specifically include contracts with third parties providing Cloud storage or processing services.	High	As at 6a/b	30 September 2018
7. Process analysis			
7a) WMCA must review all processes to ensure each of the data processing principles is established for each process. Having a lawful basis for processing personal data is a key area of compliance. Interviews identified where processes may have issues and risks associated, such as the risk of retaining personal data for longer than is necessary for the purposes for which it was collected.	High	Departmental/Team Information Asset Registers have been drafted to address effective process analysis. As with many organisations this is a new concept and will be subject to review, development, and improvement.	31 December 2018
7b) WMCA must carry out a thorough check to ensure the lawful bases identified for processing in the Process Analysis worksheet provided are valid (Articles 6 and 9). The European Commission's model standard contractual clauses or other adequate protection must be in place in respect of the contracts governing all cross-border transfers of personal data out of the EEA (Articles 44–49).	High	As at 7a (above)	31 December 2018
7c) WMCA will need to address the delay in issuing fair processing/privacy notices to data subjects, e.g. staff at new customers providing their personal details to allow the new customer to be set up. Article 13 of the GDPR states that the notice must be provided "at the time personal data are obtained".	High	As at 7a (above)	31 December 2018

7d) The duty to serve an Article 14 notice (which informs data subjects about the processing of their personal data received from third parties) sets a particular challenge. To address this, WMCA will need to put in place a procedure so that when the personal data of individuals is received from a third party (e.g. a recruitment agency), the notice is sent to those data subjects.	High	As at 7a (above)	31 December 2018
8. PIMS – Personal Information Management System			
8a) WMCA must review its documentation to ensure the authority is able to manage and demonstrate compliance with the requirements of the GDPR. It was agreed that policy management could be improved. The importance of having an inventory of processing was stressed during interviews. IT Governance's EU GDPR Documentation Toolkit would assist WMCA in generating the suite of PIMS documentation that it requires.	High	The Information Assurance Framework 'sets the stage' for necessary GDPR compliance and a suit of policies has been drafted. The relevant documentation required by Article 30 of GDPR have all been completed. We are currently working on the future review process for these polices and the dissemination of this information across the WMCA	30 November 2018
8b) It is likely that a non-GDPR-compliant form of the prescribed Article 13 notice is currently provided to WMCA staff in the authority's standard employee contract. Fully compliant Article 13 privacy notices should be standardised and issued consistently whenever personal data is collected by the authority from the data subjects themselves, as detailed in 7c above. Consent cannot be relied upon as a condition for processing employees' personal data as the employer-employee relationship is not considered to be equal; an alternative lawful basis for processing employee information will be required and will need to be put in place with all employees before 25 May 2018.	High	All article 13 notices including internal HR notices have been redrafted by the DPO and are now in use. Consent is not relied upon as a ground for processing personal data and the DPO in conjunction with the HR department have revised the ground for processing such data. Article 13 notices have been built into the WMCA data transparency commitment.	Closed
8c) Article 14 notices on the collection of personal data from third parties are not currently issued. A consistent process to remedy this gap is needed as detailed in 7d above.	High	Article 14 notices are now in place Article 14 notices have been built into the WMCA data transparency commitment.	Closed
8d) The handling and obtaining of consent will change significantly with the introduction of the GDPR (Articles 6, 7 and 9). WMCA needs to modify its existing consent processes to comply with the Regulation, recognising that consent by default will be illegal and that the right to withdraw consent accompanies the granting of consent.	High	All grounds for processing personal data have been reviewed. On the advice of the DPO consent as a legal ground has been removed in a number of areas, and a more appropriate GDPR ground has been established.	Closed

		In the limited areas where the WMCA now relies on consent it has been reviewed to ensure GDPR compliance.	
8e) WMCA should introduce a data classification scheme to quickly identify documents or data containing personal and/or highly sensitive information. This will allow employees to handle this information appropriately.	High	WMCA has adopted the Government Security Classification (GSC). An Internal Classification policy has been written and published. GSC training is included within new starter/annual data protection and Information Security education and awareness programme.	Closed
8f) WMCA should implement a GDPR-compliant data retention policy, in writing, detailing retention periods and ensuring all personal data is anonymised or securely deleted as soon as it is no longer lawful to retain it.	High	An archive and retention project group has been established to find solutions in this area and establish a modern retention & archiving process. As part of this the current policy will be reviewed and amended.	31 December 2018
8g) WMCA should ensure its formal change management process includes provisions for DPIAs (see 8j below) to be completed whenever processing of personal data is introduced or modified.	High	Data Privacy Impact Assessments (DIPA) are now part of WMCA project management where it involves processing personal data. A DPIA template and supporting guidance has been published	31 December 2018
8h) WMCA should create and maintain a record of personal data processing activities (see 6c above) under its Article 30 responsibility.	High	As at Section 7	31 December 2018
8i) The process covering the handling of SARs should be updated to meet the GDPR's increased requirements in this regard (Article 15). Reporting should be set up to ensure the relevant SAR response times are met, and in respect of the other data subject rights referred to in 10 below. All areas of the authority should be made aware of this process.	High	The process has been updated both externally and internally to meet the GDPR standard.	Closed
8j) Article 35 contains the GDPR's requirements for when a DPIA must be undertaken. The format of any security assessments or privacy impact assessments already carried out by WMCA will need to be adjusted to meet the GDPR's requirements for DPIAs. The need for work on consistency with the GDPR is likely.	High	As at 8g (above)	31 December 2018
9. ISMS			
9a) WMCA stated that it is looking at obtaining ISO 27001 certification in the future. ISO 27001 certification demonstrates that technical and organisational measures are in place to ensure there is adequate security of personal data held in hard copy or electronic form, or processed through the authority's	Medium	Attaining ISO 27001 and CE+ is a WMCA IA objective This work is ongoing and being led by the WMCA Cyber Security Specialist	31 December 2018

systems. This includes a review of methodologies for testing security, and established cyber security certifications, standards and codes of practice. During the interviews we suggested that WMCA looks into adopting the BS 10012 standard, as it is specifically geared towards GDPR compliance. During the interviews information was provided on other relevant certifications, such as Cyber Essentials and Cyber Essentials Plus. These are being established as industry standards and some organisations are expressing a preference for them.			
9b) Encryption to the current recognised industry standard should be applied to all personal data at rest and in transit to ensure accidental data loss or data loss due to malicious activity, does not lead to disclosure. Where this is currently impossible because of the use of legacy software or systems, WMCA should develop and implement a plan to upgrade these systems to include encryption as soon as possible.	High	Data at rest and in transit encryption is a baseline standard of GSC (adopted by WMCA) is OFFICIAL information. Presuming all personal information will be at least OFFICIAL, this requirement is technically achieved.	31 December 2018
9d) WMCA should ensure employees are aware of the possibility to encrypt emails end to end and apply this to any emails containing personal data. Where this is currently impossible because suppliers/third parties do not support this, WMCA should continue to use a solution that provides secure file transfers for personal data (SFTP).	Medium	As at 9b. GSC allows a given handler to risk assess their processing of relevant data and apply baseline standards accordingly.	31 December 2018
9e) WMCA should ensure any policy concerning information security explicitly references the security of data subjects, as well as penetration/security testing.	Medium	As at 9b. Annual Penetration/Vulnerability testing of all relevant systems is conducted, as a BAU activity, by WMCA ICT.	Closed
9f) Logging and monitoring processes should be assessed to make sure access to personal data is logged and monitored to prevent abusive or excessive access, and to detect data breaches or cyber-attacks.	Medium	In accordance with the Information Security Policy, all users are afforded access as per their specific job role and relevancy. ACL are controlled through AD and application level authentication. Intrusion or cyber-attacks are monitored and prevented using robust anti-intrusion techniques and tools. Strictly speaking an auditing function is not currently employed across all relevant systems and assets. This forms part of the creation of an IAR and continuing service improvement.	30 November 2018

9g) WMCA's IT security roadmap should be reviewed to ensure the security of personal data/data subjects is considered, including by way of pseudonymisation or anonymisation.	Medium	Privacy by design is a consideration through the life cycle of all systems and information assets. The application, of these measures, in accordance with the draft IM Strategy, is the responsibility of the Information Asset Owners and all system users. The DPO is available for advice and guidance, and will be incorporated with the training and awareness programme.	Closed
10. Rights of data subjects			
10a) WMCA does not have a written SAR policy or procedure. WMCA needs processes that will allow it to both facilitate and respond to data subjects exercising any or all of their rights. During the interviews the importance of the enhanced rights of data subjects under the GDPR was repeatedly stressed.	Very high	We have externally published the process for data subjects: https://www.wmca.org.uk/freedom-of-information Internal Process is managed by DPO and the internal process is documented on the WMCA intranet	Closed
10b) WMCA should implement processes (automated, if possible) to ensure it can guarantee the rights of data subjects, especially the rights to rectification and erasure. Processes should also be put in place to handle requests pursuant to the right to be informed (see 8b and 8c above), and the rights to object, to erasure and to data portability.	High	All data subject rights are explained externally and how they can be exercised. Internally the DPO manages request to exercise a data subject right. The process is documented on the WMCA intranet. New or amended systems which process personal data are designed to aid the delivery of data subject rights.	Closed

This page is intentionally left blank

Audit, Risk & Assurance Committee

Date	21 September 2018
Report title	Internal Audit Update
Accountable Chief Executive	Deborah Cadman, West Midlands Combined Authority email: deborah.cadman@wmca.org.uk tel: (0121) 214 7200
Accountable Employee	Tim Martin, Chief Audit Executive email: tim.martin@wmca.org.uk tel: (0121) 214 7435
Report to be/has been considered by	Not applicable

Recommendation(s) for action or decision:

The Audit, Risk and Assurance Committee is recommended to:

(1) Note the contents of the latest Internal Audit Update Report.

1.0 Purpose

1.1 The purpose of this report is to present the Committee with an update on the work completed by internal audit so far, this financial year.

2.0 Background

2.1 In accordance with the agreed work programme for internal audit, the reports provide an independent and objective opinion on the Combined Authority's effectiveness in managing their risk management, governance and control environment.

2.2 The reports will also feed into the Annual Internal Audit Report that will be prepared at the end of the financial year. The Annual Report will provide an overall audit opinion on the adequacy and effectiveness of the governance, risk management and internal control processes, based upon the outcome of the reviews completed during the year. This opinion can then be used to feed into the Combined Authority's Annual Governance Statement that accompanies the Annual Statement of Accounts.

3.0 Wider WMCA Implications

3.1 There are no implications

4.0 Financial implications

4.1 There are no implications

5.0 Legal implications

5.1 There are no implications

6.0 Equalities implications

6.1 There are no implications

7.0 Other implications

7.1 Not applicable

8.0 Schedule of background papers

8.1 None

9.0 Appendices

Internal Audit Update Report Quarter 2 2018-2019

Delivered by City of Wolverhampton Council – Audit Services

1 *Introduction*

The purpose of this report is to bring the Audit and Risk Assurance Committee up to date with the progress made against the delivery of the 2018 - 2019 internal audit plan.

The Audit, Risk and Assurance Committee has a responsibility to review the effectiveness of the system of internal controls and to monitor arrangements in place relating to corporate governance and risk management arrangements. Internal audit is an assurance function which provides an independent and objective opinion to the organisation on the control environment, comprising risk management, control and governance. This work update provides the committee with information on recent audit work that has been carried out to assist them in discharging their responsibility by giving the necessary assurances on the system of internal control.

The information included in this progress report will feed into and inform our overall opinion in our internal audit annual report issued at the year end. Where appropriate each report we issue during the year is given an overall opinion based on the following criteria:

Limited	Satisfactory	Substantial
There is a risk of objectives not being met due to serious control failings.	A framework of controls is in place, but controls need to be strengthened further.	There is a robust framework of controls which are applied continuously.

2 *Summary of progress*

The following reviews from the Internal Audit Plan are underway:

- Health and Safety (draft report issued)
- Asset Management (draft report issued)
- Business Continuity (fieldwork in progress)

The remaining reviews from the Internal Audit Plan for 2018 - 2019 are as follows:

- Human Resource Planning, Capacity and Capability Strategy (to be confirmed with newly appointed Head of Organisational Development)
- Devolution Deal Objectives and Financial Assumptions (postponed – update to be received in October regarding commencement)
- Business Planning (postponed – update to be received in October regarding commencement)
- Budget Management Role and Responsibilities (scheduled for quarter 3)
- Joint Data Team Initiative (scheduled for quarter 3)

- Key Financial Systems (scheduled for October 2018)
  - Payroll
  - Accounts Payable
  - Accounts Receivable
  - General Ledger
  - Budgetary Control
  - Treasury Management

- Birmingham Eastside Extension Project (scheduled for quarter 3)

- Governance Arrangements (scheduled for quarter 3)

- Midland Metro Operational Transfer (scheduled for quarter 4)

Follow up of previous recommendations

We continue to monitor the implementation of previous key recommendations, and any major issues of concern relating to their non-implementation, will be reported back to the Audit, Risk and Assurance Committee.

We are currently following up the 2017-2018 Transport for West Midlands Capital Programme Prioritisation audit.

The following 2017-18 audits will be followed up later in the year:

- Programme Management Office Project Appraisal and Support Functions
- Investment Programme – Governance Arrangements for Project Appraisal and Approval
- WMCA Key Financial Systems (to be followed up as part of 2018-2019 Key Financial Systems audits)
- IR35
- National Fraud Initiative
- Establishment of the Mayoral Office
- Data Security Arrangements (including GDPR readiness)

This page is intentionally left blank

Audit, Risk & Assurance Committee

Date	21 September 2018
Report title	Self-Assessment Exercise
Accountable Chief Executive	Deborah Cadman, West Midlands Combined Authority email: deborah.cadman@wnca.org.uk tel: (0121) 214 7200
Accountable Employee	Tim Martin, Chief Audit Executive email: tim.martin@wmca.org.uk tel: (0121) 214 7435
Report to be/has been considered by	

Recommendation(s) for action or decision:

The Audit, Risk & Assurance Committee is recommended to:

(1) Complete the following three documents as part of the self-assessment exercise:

- Self-Assessment of Good Practice
- Knowledge and Skills Framework
- Evaluating the Effectiveness of the Audit, Risk and Assurance Committee

1.0 Purpose

1.1 The Chartered Institute of Public Finance and Accountancy (CIPFA) in their Audit Committees – Practical Guidance for Local Authorities, recommend that an Audit Committee should carry out a regular review of its performance and effectiveness, alongside other self-assessment activities. As part of this process, members of the Committee are asked to complete the attached three documents:

- Self-Assessment of Good Practice
- Knowledge and Skills Framework
- Evaluating the Effectiveness of the Audit, Risk and Assurance Committee

2.0 Background

2.1 This self-assessment exercise is in line with CIPFA's Audit Committees – Practical Guidance for Local Authorities. The results will be anonymised, summarised and presented at a future meeting. The results will also help inform a structured future training programme.

3.0 Wider WMCA Implications

3.1 There are no implications

4.0 Financial implications

4.1 There are no implications

5.0 Legal implications

5.1 There are no implications

6.0 Equalities implications

6.1 There are no implications

7.0 Other implications

7.1 Not applicable

8.0 Schedule of background papers

8.1 None

9.0 Appendices

West Midlands Combined Authority

Audit, Risk and Assurance Committee: Self-assessment of Good Practice

Completed by ……. Date: ……

Good practice questions	Yes	Partly	No
Audit, Risk and Assurance Committee purpose and governance			
Does the Authority have a dedicated audit committee?			
Does the committee report directly to the Authority?			
Do the terms of reference clearly set out the purpose of the committee in accordance with CIPFA's Position Statement (see below)?			
Is the role and purpose of the committee understood and accepted across the Authority?			
Does the committee provide support to the Authority in meeting the requirements of good governance?			
Are the arrangements to hold the committee to account for its performance operating satisfactorily?			
Functions of the committee			
Do the committee's terms of reference explicitly address all the core areas identified in CIPFA's Position Statement? • Good governance • Assurance framework, including partnerships and collaboration arrangements • Internal audit • External audit • Financial reporting • Risk management • Value for money or best value • Counter-fraud and corruption • Supporting the ethical framework			
Is an annual evaluation undertaken to assess whether the committee is fulfilling its terms of reference and that adequate consideration has been given to all core areas?			
Has the committee considered the wider areas identified in CIPFA's Position Statement and whether it would be appropriate for the committee to undertake them?			
Where coverage of core areas has been found to be limited, are plans in			

place to address this?			
Has the committee maintained its non-advisory role by not taking on any decision-making powers that are not in line with its core purpose?			
Membership and support			
Has an effective committee structure and composition of the committee been selected? This should include: • Separation from the executive • An appropriate mix of knowledge and skills among the membership • A size of committee that is not unwieldy • Consideration has been given to the inclusion of at least one independent member (where it is not already a mandatory requirement)			
Have independent members appointed to the committee been recruited in an open and transparent way and approved by the full Authority?			
Does the chair of the committee have appropriate knowledge and skills?			
Are arrangements in place to support the committee with briefings and training?			
Has the membership of the committee been assessed against the core knowledge and skills framework and found to be satisfactory?			
Does the committee have good working relations with key people and organisations, including external audit, internal audit and the chief financial officer?			
Is adequate secretariat and administrative support to the committee provided?			
Has the committee obtained feedback on its performance from those interacting with the committee or relying on its work?			
Are meetings effective with a good level of discussion and engagement from all members?			
Does the committee engage with a wide range of leaders and mangers, including discussion of audit findings, risks and action plans with responsible officers?			
Does the committee make recommendations for the improvement of governance, risk and control and are these acted on?			
Has the committee evaluated whether and how it is adding value to the organisation?			
Does the committee have an action plan to improve any areas of weakness?			
Does the committee publish an annual report to account for its performance and explain its work?			

CIPFA's Position Statement: Audit Committees in Local Authorities

The scope of this Position Statement includes all principal local authorities in the UK, the audit committees for PCCs and chief constables in England and Wales, and the audit committees of fire and rescue authorities.

1 Audit committees are a key component of an authority's governance framework. Their function is to provide an independent and high-level resource to support good governance and strong public financial management.

2 The purpose of an audit committee is to provide to those charged with governance independent assurance on the adequacy of the risk management framework, the internal control environment and the integrity of the financial reporting and governance processes. By overseeing both internal and external audit it makes an important contribution to ensuring that effective assurance arrangements are in place.

3 Authorities and police audit committees should adopt a model that establishes the committee as independent and effective. The committee should:

- act as the principal non-executive, advisory function supporting those charged with governance
- in local authorities, be independent of both the executive and the scrutiny functions and include an independent member where not already required to do so by legislation
- in police bodies, be independent of the executive or operational responsibilities of the PCC or chief constable
- have clear rights of access to other committees/functions, for example, scrutiny and service committees, corporate risk management boards and other strategic groups
- be directly accountable to the authority's governing body or the PCC and chief constable.

4 The core functions of an audit committee are to:

- be satisfied that the authority's assurance statements, including the annual governance statement, properly reflect the risk environment and any actions required to improve it, and demonstrate how governance supports the achievement of the authority's objectives
- in relation to the authority's internal audit functions: oversee its independence, objectivity, performance and professionalism, support the effectiveness of the internal audit process and promote the effective use of internal audit within the assurance framework
- consider the effectiveness of the authority's risk management arrangements and the control environment, reviewing the risk profile of the organisation and assurances that action is being taken on risk-related issues, including partnerships and collaborations with other organisations
- monitor the effectiveness of the control environment, including arrangements for ensuring value for money, supporting standards and ethics

and for managing the authority's exposure to the risks of fraud and corruption

- consider the reports and recommendations of external audit and inspection agencies and their implications for governance, risk management or control
- support effective relationships between external audit and internal audit, inspection agencies and other relevant bodies, and encourage the active promotion of the value of the audit process.
- review the financial statements, external auditor's opinion and reports to members, and monitor management action in response to the issues raised by external audit.

5 An audit committee can also support its authority by undertaking a wider role in other areas including:

- considering governance, risk or control matters at the request of other committees or statutory officers
- working with local standards and ethics committees to support ethical values
- reviewing and monitoring treasury management arrangements in accordance with Treasury Management in the Public Services: Code of Practice and Cross-Sectoral Guidance Notes (CIPFA, 2017)
- providing oversight of other public reports, such as the annual report.

6 Good audit committees are characterised by:

- a membership that is balanced, objective, independent of mind, knowledgeable and properly trained to fulfil their role. The political balance of a formal committee of a council will reflect the political balance of the council, however, it is important to achieve the right mix of apolitical expertise
- a membership that is supportive of good governance principles and their practical application towards the achievement of organisational objectives
- a strong independently minded chair – displaying a depth of knowledge, skills and interest. There are many personal qualities needed to be an effective chair, but key to these are promoting apolitical open discussion, managing meetings to cover all business and encouraging a candid approach from all participants, an interest in and knowledge of financial and risk management, audit, accounting concepts and standards, and the regulatory regime
- unbiased attitudes – treating auditors, the executive and management fairly
- the ability to challenge the executive and senior managers when required.

7 To discharge its responsibilities effectively the committee should:

- meet regularly – at least four times a year, and have a clear policy on those items to be considered in private and those to be considered in public
- be able to meet privately and separately with the external auditor and with the head of internal audit
- include, as regular attendees, the CFO(s), the chief executive, the head of internal audit and the appointed external auditor. Other attendees may include the monitoring officer (for standards issues) and the head of resources (where such a post exists). These officers should also be able to access the committee, or the chair, as required
- have the right to call any other officers or agencies of the authority as required, while recognising the independence of the chief constable in relation to operational policing matters
- report regularly on its work to those charged with governance, and at least annually report an assessment of their performance. An annual public report should demonstrate how the committee has discharged its responsibilities.

This page is intentionally left blank

West Midlands Combined Authority

Evaluating the effectiveness of the Audit, Risk and Assurance Committee

Key	
5	Clear evidence is available from a number of sources that the committee is actively supporting improvements across all aspects of this area. The improvements made are clearly identifiable.
4	Clear evidence from some sources that the committee is actively and effectively supporting improvement across some aspects of this area
3	The committee has had mixed experience in supporting improvement in this area. There is some evidence that demonstrates their impact but there are also significant gaps
2	There is some evidence that the committee has supported improvements, but the impact of this support is limited.
1	No evidence can be found that the audit committee has supported improvements in this area.

Areas where the committee can add value by supporting improvement	Examples of how the committee can add value and provide evidence of effectiveness	Self-evaluation examples – areas of strength and weakness	Overall assessment 5 – 1
Promoting the principles of good governance and their application to decision making	Supporting the development of a local code pf governance. Providing robust review of the AGS and the assurances underpinning it. Working with key members/ governors to improve their understanding of the AGS and their contribution to it. Supporting review/audits of governance arrangements. Participating in self-assessments of governance arrangements.		

	Working with partner audit committees to review governance arrangements in partnerships.		
Contributing to the development of an effective control environment	Monitoring the implementation of recommendations from auditors. Encouraging ownership of the internal control framework by appropriate managers. Raising significant concerns over controls with appropriate senior managers.		
Supporting the establishment of arrangements for the governance of risk and for effective arrangements to manage risks.	Reviewing risk management arrangements and their effectiveness, e.g. risk management benchmarking. Monitoring improvements. Holding risk owners to account for major / strategic risks.		
Advising on the adequacy of the assurance framework and considering whether assurance is deployed efficiently and effectively.	Specifying its assurance needs, identifying gaps or overlaps in assurance. Seeing to streamline assurance gathering and reporting. Reviewing the effectiveness of assurance providers, e.g. internal audit, risk management, external audit.		
Supporting the quality of the internal audit activity, particularly by underpinning its organisational independence	Reviewing the audit charter and functional reporting arrangements. Assessing the effectiveness of internal audit arrangements and supporting improvements. Actively supporting the quality assurance and improvement programme of internal audit.		

Aiding the achievement of the authority's goals and objectives through helping to ensure appropriate governance, risk, control and assurance arrangements.	Reviewing how the governance arrangements support the achievement of sustainable outcomes. Reviewing major projects and programmes to ensure that governance and assurance arrangements are in place. Reviewing the effectiveness of performance management arrangements.		
Supporting the development of robust arrangements for ensuring value for money.	Ensuring that assurance on value for money arrangements is included in the assurances received by the audit committee. Considering how performance in value for money is evaluated as part of the AGS.		
Helping the authority to implement the values of good governance, including effective arrangements for countering fraud and corruption risks.	Reviewing arrangement against the standards set out in CIPFA's Code of Practice on Managing the Risk of Fraud and Corruption. Reviewing fraud risks and the effectiveness of the organisation's strategy to address those risks. Assessing the effectiveness of ethical governance arrangements for both staff and governors.		
Promoting effective public reporting to the authority's stakeholders and local community and measures to improve transparency and accountability	Improving how the authority discharges its responsibilities for public reporting; for example, better targeting at the audience, plain English. Reviewing whether decision making through partnership organisations remains transparent and publicly accessible and encouraging greater transparency. Publishing an annual report from the committee.		

This page is intentionally left blank

West Midlands Combined Authority

Audit, Risk and Assurance Committee Members: Knowledge and Skills Framework

Completed by …… Date …….

Core areas of knowledge

Knowledge Area	Details of core knowledge required	How the committee member is able to apply the knowledge	Audit Committee Member ranking (score between 5 = strong to 1 = minimal)
Organisational knowledge	An overview of the governance structures of the authority and decision-making processes. Knowledge of the organisational objectives and major functions of the authority	This knowledge will be core to most activities of the committee including review of the Annual Governance Statement, internal and external audit reports and risk registers.	
Audit Committee role and functions	An understanding of the committee's role and place within the governance structures. Familiarity with the committee's terms of reference and accountability arrangements. Knowledge of the purpose and role of the committee	This knowledge will enable the committee to prioritise its work in order to ensure it discharges its responsibilities under its terms of reference and to avoid overlapping the work of others.	

Governance	Knowledge of the seven principles of the CIPFA/SOLACE Good Governance Framework and the requirements of the Annual Governance Statement (AGS). Knowledge of the local code of governance	The committee will review the local code of governance and consider how governance arrangements will align to the principles in the framework. The committee will plan the assurances it is to receive in order to adequately support the AGS. The committee will review the AGS and consider how the authority is meeting the principles of good governance.	
Internal audit	An awareness of the key principles of the *Public Sector Internal Audit Standards* and the *local Government Application Note.* Knowledge of the arrangements for delivery of the internal audit service in the authority and how the role of the head of internal audit is fulfilled.	The committee has oversight of the internal audit function and will monitor its adherence to professional internal audit standards. The committee will review the assurances from internal audit work and will review the risk-based audit plan. The committee will also receive the annual report, including an opinion and information on conformance with professional standards. In relying on the work of internal audit, the committee will need to be confident that professional standards are being followed. The audit committee chair is likely to be interviewed as part of the external quality assessment and the committee will receive the outcome of the assessment and action plan.	
Financial management and accounting	Awareness of the financial statement that the authority must produce and the principles it must follow to produce them. Understanding of good financial management principles. Knowledge of how the organisation meets the requirements of the role of the chief financial officer, as required by the *CIPFA Statement on the Role of the Chief Financial officer in Local Government.*	Reviewing the financial statements prior to publication asking questions. Receiving the external audit report and opinion on the financial audit. Reviewing both external and internal audit recommendations relating to financial management and controls. The committee should consider the role of the CFO and how this is met when reviewing the AGS.	
External Audit	Knowledge of the role and functions of the external auditor and who currently undertake this role.	The committee should meet with the external auditor regularly and receive their reports and opinions. Monitoring external audit recommendations and maximising benefit from audit process.	

	Knowledge of the key reports and assurances that external audit will provide. Knowledge about arrangements for the appointment of auditors and quality monitoring undertaken.	The committee should monitor the relationship between the external auditor and the authority and support the delivery of an effective service.	

Risk management	Understanding of the principles of risk management, including linkage to good governance and decision making. Knowledge of the risk management policy and strategy of the organisation. Understanding of risk governance arrangements, including the role of members and of the committee.	In reviewing the AGS, the committee will consider the robustness of the authority's risk management arrangements and should also have awareness of the major risks the authority faces. Keeping up to date with the risk profile is necessary to support the review of a number of committee agenda items, including the risk-based internal audit plan, external audit plans and the explanatory foreword of the accounts. Typically, risk registers will be used to inform the committee. The committee should also review reports and action plans to develop the application of risk management practice.	
Counter- fraud	An understanding of the main areas of fraud risk the organisation is exposed to. Knowledge of the principles of good fraud risk management in accordance with the Code of Practice on Managing the Risk of Fraud and Corruption. Knowledge of the organisation's arrangements for tackling fraud.	Knowledge of fraud risks and good fraud risk management practice will be helpful when the committee reviews the organisation's fraud strategy and receives reports on the effectiveness of that strategy. An assessment of arrangements should support the AGS and knowledge of good fraud risk management practice will support the Audit Committee member in reviewing that assessment.	
Values of good governance	Knowledge of the Seven Principles of Public Life. Knowledge of the authority's key arrangements to uphold ethical standards for both members and staff. Knowledge of the whistleblowing arrangements in the authority.	The committee member will draw on this knowledge when reviewing governance issues and the AGS. Oversight of the effectiveness of whistleblowing will be considered as part of the AGS. The committee member should know to whom concerns should be reported.	
Treasury management (only if it is within the terms of reference of the committee to provide scrutiny)	Effective Scrutiny of Treasury management is an assessment tool for reviewing the arrangements for undertaking scrutiny of treasury management. The key knowledge areas identified are:	Core knowledge on treasury management is essential for the committee undertaking the role of scrutiny.	

	• Regulatory requirements • Treasury risks • The organisation's treasury management strategy • The organisation's policies and procedures in relation to treasury management		

Specialist Knowledge that adds value to the Audit, Risk and Assurance Committee

Knowledge area	Details of supplementary knowledge	How the Audit Committee member is able to add value to the committee	Audit Committee Member ranking (score between 5 = strong to 1 = minimal)
Accountancy	Professional qualification in accountancy	More able to engage with the review of the accounts and financial management issues coming before the committee. Having an understanding of the professional requirements and standards that the finance function must meet will provide helpful context for discussions of risks and resource issues. More able to engage with the external auditors and understand the results of audit work.	
Internal audit	Professional qualification in internal audit.	This would offer in-depth knowledge of professional standards of internal audit and good practice in internal auditing. The committee would be more able to provide oversight of internal audit and review the output of audit reports.	
Risk management	Risk management qualification. Practical experience of applying risk management. Knowledge or risks and opportunities associated with major areas of activity.	Enhanced knowledge of risk management will inform the committee's oversight of the development of risk management practice. Enhanced knowledge of risks and opportunities will be helpful when reviewing risk registers.	

Governance and legal	Legal qualification and knowledge of specific areas of interest to the committee, for example constitutional arrangements, data protection or contract law.	Legal knowledge may add value when the committee considers areas of legal, risk or governance issues.	
Service knowledge relevant to the functions of the organisation	Direct experience of managing or working in a service area similar to that operated by the authority. Previous Scrutiny Committee experience.	Knowledge of relevant legislation, risks and challenges associated with major service areas will help the committee to understand the operational context.	
Programme and project management	Project management qualifications or practical knowledge of project management principles.	Expert knowledge in this area will be helpful when considering project risk management or internal audit reviews.	
IT systems and IT governance	Knowledge gained form management or development work in IT.	Knowledge in this area will be helpful when considering IT governance arrangements or audit reviews of risks and controls.	

Core Skills

Skills	Key elements	How the Audit Committee member is able to apply the skill	Audit Committee Member ranking (score between 5 = strong to 1 = minimal)
Strategic thinking and understanding of materiality	Able to focus on material issues and overall position, rather than being side-tracked by detail	When reviewing audit reports, findings will include areas of higher risk, or materiality to the organisation, but may also contain more minor errors or control failures. The committee member will need to pitch its review at an appropriate level to avoid spending too much time on detail.	
Questioning and constructive challenge	Able to frame questions that draw out relevant facts and explanations. Challenging performance and seeking explanation while avoiding hostility or grandstanding.	The committee will review reports and recommendations to address weaknesses in internal control. The committee member will seek to understand the reasons for weaknesses and ensure a solution is found.	

Focus on improvement	Ensuring there is a clear plan of action and allocation of responsibility	The outcome of the committee will be to secure improvements to the governance, risk management or control of the organisation, including clearly defined actions and responsibilities. Where errors or control failures have occurred, then the committee should seek assurances that appropriate action has been taken.	
Able to balance practicality against theory	Able to understand the practical implications of recommendations to understand how they might work in practice.	The committee should seek assurances that planned actions are practical and realistic.	
Clear communication skills and focus on the needs of users	Support the use of plain English in communications, avoiding jargon, acronyms, etc.	The committee will seek to ensure that external documents such as the Annual Governance Statement and the explanatory foreword to the accounts are well written for a non-expert audience.	
Objectivity	Evaluate information on the basis of evidence presented and avoiding bias or subjectivity.	The committee will receive assurance reports and review risk registers. There may be differences of opinion about the significance of risk and the appropriate control responses and the committee member will need to weigh up differing views.	
Meeting management skills	Chair the meeting effectively: summarise issues raised, ensure all participants are able to contribute, focus on the outcome and actions from the meeting.	These skills are essential for the committee chair to help ensure that meetings stay on track and address the items on the agenda. The skills are desirable for all other members.	

This page is intentionally left blank