



Audit, Risk and Assurance Committee Meeting

Date	29 September 2021
Report title	Internal Audit Update – September 2021
Accountable Chief Executive	Laura Shoaf, Interim Chief Executive
Accountable Employee	Satish Mistry, Interim Director, Law and Governance
Report has been considered by	Strategic Leadership Team

Recommendation(s) for action or decision:

The Combined Authority Audit, Risk and Assurance Committee is recommended to:

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

9.1 None

This report is PUBLIC [NOT PROTECTIVELY MARKED]



West Midlands Combined Authority

**Internal Audit Update Report – September 2021
2021-2022**

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 2021 - 2022 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:

No Assurance	Limited	Satisfactory	Substantial
Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

2 Summary of progress:

The following internal audit reviews have been completed or are currently underway.

Auditable area	AAN Rating	Status and level of assurance	ARAC Meeting (indicative)
2020-2021 Internal Audit Reviews previously reported (will feed into the 2021-2022 opinion)			
Commonwealth Games Transport Plan – TfWM Governance and Management Arrangements	High	Final Issued - Substantial	June 2021
Risk Management	High	Final Issued - Satisfactory	June 2021
Digital Retraining Fund	High	Final Issued - Satisfactory	June 2021
2020-2021 Internal Audit Reviews completed			
Adult Education Budget (appended)	High	Final Issued - Satisfactory	September 2021

Auditable area	AAN Rating	Status and level of assurance	ARAC Meeting (indicative)
2021-2022 Internal Audit Reviews completed			
General Data Protection Regulations (appended)	High	Final Issued – Satisfactory	September 2021
Corporate Complaints Process	High	Draft Issued - Satisfactory	November 2021
2021-2022 Internal Audit Reviews in progress			
TfWM COVID 19 Response – Management and Decision-Making Arrangements	High	Fieldwork in progress	November 2021
Single Commissioning Framework - Land Fund	High	Fieldwork in progress	November 2021
Freedom of Information	High	Fieldwork in progress	November 2021
WMCA Key Financial Systems	High	Planning commenced	January 2022
Dudley Interchange	Medium	Planning commenced	January 2022
Longbridge Park and Ride Income Management and Charging Arrangements	Medium	Planning commenced	April 2022

3 Forward plan for 2021-2022 scheduled audits

Auditable area	AAN Rating	Quarter	ARAC Meeting (indicative)
Bid Management Framework	High	Awaiting WMCA response regarding rescheduling	
Local Industrial and Economic Strategy	High	Awaiting WMCA decision regarding deferral	
WM2041 Delivery Programme (Environmental Recovery)	High	Deferred by WMCA – January 2021	April 2022
Affordable Housing Delivery Vehicle	High	3	April 2022
ICT Strategy	High	3	April 2022
Inclusive Growth Investment Toolkit	High	4	April 2022
Investment Programme Monitoring and Evaluation Arrangements	High	4	June 2022
Adult Education Budget	High	4	June 2022

4 Follow-up of previous recommendations

Through an ongoing cycle of reviews, 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.

As part of a new working arrangement, the WMCA Internal Audit Liaison Officer will be undertaking the initial preparatory work for each follow-up review, obtaining progress updates, and supporting evidence as and when agreed implementation dates arrive. This is in support also of the WMCA management monitoring arrangements of progress with implementation.

Internal Audit upon referral from the Internal Audit Liaison Officer, will then independently review the progress and supporting evidence, and report accordingly on the progress made with implementation of recommendations. Ultimately, Internal Audit will retain the responsibility for determining if sufficient action has been taken.

Follow up action of the following reviews forms part of this ongoing cycle:

Auditable area	Overall Opinion	Agreed Actions			Number Implemented
		Red	Amber	Green	
Completed					
Devolution Deal Objectives and Financial Assumptions, including Business Planning (summary below)	Final issued - Satisfactory	-	2	-	Action still in progress
In progress (Internal Audit Liaison Officer)					
Third Generation Tram Procurement Project Management	Satisfactory	-	2	3	-
Sprint Programme Management Arrangements	Substantial	-	-	4	-
Midland Metro Limited Operational Transfer	Satisfactory	-	2	-	-
West Midlands Rail Limited - WMCA Governance and Management Arrangements	Satisfactory	-	3	-	-
Forward plan					
Programme and Project Management Framework	Satisfactory	-	3	-	-
WMCA Accessible Transport Services	N/A	-	4	2	-
Environmental Management System	Satisfactory	-	1	1	-
Human Resources Pre-employment checks	N/A	-	2	-	-

Auditable area	Overall Opinion	Agreed Actions			Number
Procurement (Covid-19 Response)	Substantial	-	-	1	-
Harvesttime Project Management Arrangements	Substantial	-	-	5	-
Risk Management	Satisfactory	-	1	3	-
Digital Retraining Fund	Satisfactory	-	3	1	-
Commonwealth Games Transport Plan - TfWM Governance and Management Arrangements	Substantial	-	-	3	-
Deferred					
WMCA Governance Arrangements*	Substantial	-	-	6	-
Employee Performance Management#	Satisfactory	-	1	1	-

Summary

Devolution Deal Objectives and Financial Assumptions, including Business Planning (2019)

We sought assurance that appropriate performance management and business planning arrangements had been established. Two amber recommendations were made for implementation by December 2019 regarding the establishment of an organisational wide performance management framework and revision of the business planning tool to better support performance monitoring and reporting.

However, at the time of our review the amber recommendations were yet to be implemented. Action was still ongoing as part of development of the WMCA's approach to performance management and monitoring, and business planning to meet a new Corporate Strategy (September 2021 for implementation through the 2022-2023 Annual Plan), the Annual Plan, and newly defined High-Level Deliverables.

Both amber recommendations had been reiterated as they remain relevant within the above developmental work with a revised implementation date of March 2022.

* WMCA advised a detailed review is proposed of governance arrangements post mayoral elections and a full audit will be undertaken in due course

#Due to implementation of a revised framework a full audit is recommended in 2022-2023 once the new arrangements are embedded.



West Midlands Combined Authority

Final Internal Audit Report: WMCA Devolved Adult Education Budget 2020-2021

Report Date: 7 September 2021

Report Distribution: Julie Nugent – Director, Productivity and Skills
Clare Hatton – Head of Skills Delivery
Iris Both – Senior Delivery Manager Adult Education

Linda Horne – Finance Director (s151 Officer)
Louise Cowen – Financial Controller
Fahmida Chowdhury – Productivity and Skills Finance Business Partner
Ian Martin – Investment and Commercial Activities Director
Joti Sharma - Head of Programme Assurance & Appraisal

Satish Mistry, Interim Director, Law and Governance
Jayne Middleton – Interim Legal Services Manager

1. Executive summary

Introduction

An audit of the arrangements for the West Midlands Combined Authority (WMCA) Adult Education Budget (AEB / the Budget) was undertaken as part of the approved internal audit plan for the financial year 2020 / 2021.

Responsibility for the Budget and how it is delivered within the West Midlands region was devolved from the Department for Education (DfE) to the WMCA in August 2019. The academic year 2019 / 2020 was the first year of funding.

The Regional Skills Plan sets out the key difficulties in the local labour market with increasing importance to address such issues as low employment rate, high levels of unemployment, low wage levels leading to issues of poverty, low skills and qualification attainment, and persistent skills shortages.

The aim of the Budget is to engage adults and employers in providing the skills and learning required for the region to equip adults for work, upskill current employees and facilitate specialist training whilst aligning funding with priority individuals, communities, and sectors.

The Budget is used to fund education provision through a range of delivery providers including grant agreements with Colleges and Local Authorities across the region, and contracts with Independent Training Providers (ITPs). Of the total 62 providers, 22 Colleges, five West Midlands Local Authorities and 35 ITPs had been allocated funding for the provision of adult education within 2020 / 2021.

The total funding allocation to Colleges, Local Authorities, and ITPs for the current funding year 2020 / 2021 was £126,739,021. Colleges were allocated £76,541,502, Local Authorities £21,811,751 and ITPs £28,385,768.

The Budget is supported by the WMCA Payment and Performance Management Framework (Framework) covering key processes for undertaking performance monitoring of delivery by providers in accordance with grant agreements / contracts and for determining payments to providers based on validated learner delivery data. Integration with Education Skills Funding Agency (ESFA) processes and liaison within ESFA regimes for oversight of providers, further supports the Framework and processes established by the WMCA.

Scope and objectives of audit work

Our audit was conducted in conformance with the Public Sector Internal Audit Standards and considered the following objectives, and the potential risks to the achievement of those objectives:

- To seek assurance that effective governance and management arrangements have been established for the operation of the AEB to ensure achievement of the strategic objectives and aims regarding skills and education within the Regional Skills Plan are supported.

Scope	Potential risks
The scope of the audit included high level review of the governance and management arrangements (including performance and	<ul style="list-style-type: none"> Achievement of the strategic objectives and aims within the Regional Skills Plan may not be effectively supported by

compliance monitoring, and audit and assurance) supporting delivery of the Budget. As part of the above, reference was made (but not limited) to the following core WMCA AEB documents and processes:

- Funding Rules
- Provider Payment and Performance Management Framework
- Financial Due Diligence and Financial Health Monitoring for Independent Providers.

governance and management arrangements in place or operated.

- Effective use of the Budget may not be fully supported due to poorly operated governance and management arrangements.
- Ineffective performance, compliance and assurance arrangements may lead to a failure to prevent or detect poor or non-compliant provider performance and delivery and poor learning outcomes.
- Fraudulent use of funding may not be prevented or detected.

Limitations to the scope of our audit

The review was limited to high level coverage of the above scope. Testing was undertaken in respect of the 2020 / 2021 funding year to date for a sample of providers to cover the most current processes: one College, one Local Authority and three ITPs. Reference to 2019 / 2020 funding year was made in respect of audit and assurance arrangements and contracts / grant agreements. The sample of five providers represented a total contract / grant agreement value of £40,321,280 being 32% of the total allocation for 2020 / 2021. The College represented 29%, the Local Authority 47% and the ITPs 27% of the total allocation for each respective provider category.

Reference was made to the National Local Growth Assurance Framework (including Annex C) regarding assurance arrangements for Adult Education Budgets.

Overall conclusion

Our audit provides **satisfactory** assurance over the adequacy of the controls reviewed as part of the process to mitigate risks to an acceptable level.

No Assurance	Limited	Satisfactory	Substantial
Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

Key issues identified

We have identified three **amber** issues where improvements could be made, arising from the following:

- Sample testing identified that a signed version of an ITP contract with a value of £1,891,553 had not been retained by the WMCA and several sampled grant agreements and contracts did not indicate the date of execution.
- Documentary evidence of delegated s151 Officer approval of provider payments had not been presented at the time of payment request or retained centrally within WMCA financial records and the audit trail in support of AEB payment transactions.
- An AEB Local Assurance Framework document was yet to be established in line with the requirements of the National Local Growth Assurance Framework.

In addition, we have raised two issues classified as **green** which are detailed in section two of this report.

A copy of this report will be presented to the Audit, Risk and Assurance Committee.

Examples of good practice identified

During our work we identified the following examples of good practice in the management of risk, as achieved through the effective design and application of controls:

AEB Governance Arrangements

- Suitable governance arrangements had been established for the AEB through directorate Senior Management Team meetings and specific monthly AEB Payment Group meetings attended by AEB senior officers and the Finance Director (s151 Officer).
- Establishment of the AEB Payment Group provided appropriate governance, management oversight, performance, and financial monitoring as well as approval arrangements for AEB payments with appropriate membership and authority / delegation.
- Suitable meeting records for the AEB Payments Group meetings held between December 2020 and March 2021 were maintained for each meeting.
- AEB Payment Group minutes reflected clear discussion of risks and issues as well as achievements regards provider delivery and specifically payments due to providers prior to approval and payments being made.
- Delegation had been suitably granted and approved by the WMCA Board to the s151 Officer for authorisation of AEB payments to providers due to the amounts being routinely over and above limits within the Scheme of Delegation.
- Review of the Payments Briefings produced for the same period to support the AEB Payment Group's approval of monthly payments confirmed that they had been suitably retained and provided appropriate management information and details of payments due.
- Whilst earlier minutes referred to discussion and approval of payments due involving the s151 Officer, the minutes of the June 2021 meeting suitably and clearly evidenced approval.

- Effective arrangements had been established for delivery review and decision-making by senior officers within Productivity and Skills regarding flexibility and growth requests submitted by providers. As evidence of the decision-making undertaken, a suitably detailed decision log had been maintained showing requests, recommendations, discussions undertaken, and outcome regards whether approved or declined. The date of the decision and details of officers involved in the decision making were suitably noted. Reference to associated payments resulting from these decisions was evident within AEB Payment Group meeting records and supporting Payment Briefs.

Contracts and Grant Agreements

- The two grant agreements and three contracts / extension letters in the selected sample for 2020 / 2021 included suitable reference and links to the 2020 / 2021 Payment and Performance Management Framework via a hyperlink to the WMCA website.
- Delivery plans had been established in support of each grant agreement and contract sampled.
- Performance management arrangements suitably reflected contract/ grant agreement values and delivery plan outputs as applicable per sample testing.
- A register had been suitably maintained of all providers for 2020 / 2021 allocations detailing award type (grant or contract) and payment type (profile or actuals) and contract values.

Performance Management Arrangements

Framework and processes

- A suitably documented Payment and Performance Management Framework (Framework) was in place for each funding year including 2020 / 2021 detailing guidance to ITPs, Colleges and Local Authorities in receipt of devolved WMCA AEB for this funding year.
- The Framework suitably covers appropriate core areas: financial due diligence, data collection and validation, payment arrangements and provider performance monitoring and management review arrangements, and compliance and assurance arrangements.
- The Framework was further supported by a more detailed AEB Performance Review Framework process document outlining performance review arrangements and areas of coverage regarding delivery and compliance.
- AEB Relationship Managers and Skills Delivery Officers were allocated to each provider for the purposes of ongoing liaison as well as undertaking performance reviews at periodic points throughout the funding year as well as at the end of the year as a reconciliation exercise.

Monthly monitoring reviews

- Monthly performance monitoring arrangements had been clearly defined and established as documented within the AEB Performance Review Framework document. Monitoring activities included use of Individualised Learner Record (ILR) data submitted by providers, desk-based review as well as direct contact and liaison with providers, assisting with day to day provider queries and providing additional support such as training and guidance.
- Suitable dashboard-based Highlight Reports (HLRs) were produced covering each provider.

Reports included performance management information regarding comparison of delivery against profile / contract both in terms of funding and numbers of learners. RAG ratings for each provider were also calculated based on performance monitoring information covering overall risk and delivery performance against profile. HLRs were also used for recording and tracking actions arising from monthly reviews.

- Sample testing confirmed that HLRs had been suitably completed as above for each provider on a monthly basis. Progression of stated actions was evident between monthly reviews.

Performance management reviews

- Suitable mechanisms (i.e. reporting database and action tracking) had been established for managing and tracking progress with undertaking more in-depth periodic Performance Management Reviews (PMRs) at specific points in the funding year as well as part of year-end reconciliation. Sample testing demonstrated use of such mechanisms to ensure PMRs undertaken on a timely basis.
- Templates (for providers to complete) and meeting agenda (for the review meetings held with each provider) had been appropriately developed and clearly supported the PMR process. Templates and meeting agendas suitably covered core areas: allocations, delivery plans, destination and progression regards learners, quality, audit, and finance, subcontracting, collaboration and impact, and identification of barriers and future plans as well as review of actions.
- Sample testing for the five selected providers confirmed that a PMR report had been produced for each provider within the January 2021 round of reviews. The format of each report was in line with the templates and included all areas covered by the PMR process.
- An overall PMR report was also completed (March 2021) and suitably covered overall AEB performance and risks, with each area further broken down to coverage of grant funded providers and ITPs with key action stated as applicable.

Risk Management Arrangements

- A risk-based approach to performance monitoring and management arrangements was clearly advocated within the Framework to determine the level and frequency of review applied to each provider.

Financial Due Diligence (AEB Team / ESFA)

- The Framework suitably referenced both the WMCA's approach for financial due diligence and financial health assessments for 2020 / 2021 as well as the ESFA Financial Intervention Regime for Further Education Colleges and ESFA Oversight for ITPs. Local Authorities are deemed exempt by the ESFA.
- As well as the WMCA having its own monitoring arrangements, the WMCA and ESFA also collaborate jointly regarding monitoring and oversight of Colleges and ITPs through a series of regular meetings and as and when issues arise regarding providers funded by both the WMCA and ESFA.
- Review of meeting records confirmed that quarterly meetings were held between the WMCA AEB senior officers and the ESFA Regional Team to review and consider college and ITP provision, performance issues and any financial risks and issues flagged by either or both

organisations. Joint reviews and investigations may be commissioned as a result of issues and risks arising. Operational level meetings were also evident in support of the quarterly meetings.

- Action notes with stated owners and deadlines were suitably maintained for quarterly meetings (December 2020 and March 2021) and detailed attendees showing representation from the ESFA and WMCA. Also, actions completed from previous meetings and key actions arising were recorded.
- It is understood that ESFA derived gradings from their own financial assessments / monitoring activity for both Colleges and ITPs that are shared with ESFA funded providers are also shared with the WMCA.

Financial Due Diligence and Financial Health Monitoring for ITPs (WMCA Finance)

- The Framework suitably refers to implementation of an approach to Financial Due Diligence and Financial Health Monitoring for ITPs (the Due Diligence Guide) as operated by WMCA Finance. A revised approach was introduced in December 2020 as a result of review of previous arrangements.
- The Due Diligence Guide clearly detailed the approach and processes for assessing the financial health of and grading each ITP as well as providing guidance to ITPs regards the mandatory requirement to submit financial information by specified deadlines.
- The metrics (based on solvency, profitability and gearing ratios) and the gradings (outstanding, good, satisfactory or inadequate) utilised with the WMCA's approach clearly aligned with that used by the ESFA (Financial health guidance for organisations contracting with or applying to ESFA which relates to ITPs).
- An override facility had been included to award an automatic rating of inadequate based on failure to pass a specific number of metrics.
- Suitable details regards the frequency of monitoring and requirement for providers to submit mandatory information was also included in the Due Diligence Guide based on the grading awarded (i.e. monthly frequency for inadequate, four months for good, two for satisfactory and six for outstanding), as well as a year-end validity check.
- Finance had established a suitable spreadsheet mechanism for undertaking the above assessment and calculating gradings based on both information submitted by ITPs and other information available from credit scoring agencies and Companies House as examples.
- Arrangements were in place for informing ITPs of their assessed grading and the resultant frequency with which they must provider mandatory information.
- Sample testing for financial assessments and gradings undertaken between August 2020 and May 2021 based on the spreadsheet maintained by Finance identified that financial assessments were undertaken largely in line with the frequency defined for each grading. Testing also confirmed that providers had been suitably notified of their gradings. For the one ITP in the sample rated as inadequate monthly assessment had been evidenced in accordance with the defined frequency.

- Sampled assessments undertaken in December 2020 suitably covered the period between the initial assessment in August 2020 with assessments being undertaken on a regular basis from January 2021 onwards.

National Local Growth Assurance Framework

- The Payment and Performance Management Framework as well as supporting process / guidance documents collectively provide a suitable assurance framework for the AEB and in principle help meet the requirements of the National Local Growth Assurance Framework (Annex c) (National Assurance Framework).
- The National Assurance Framework requirement for an annual monitoring and evaluation report for AEB delivery and spend was suitably met by the WMCA in respect of 2019 / 2020.
- The report clearly included summary of delivery and spend in terms of providers, learners and aims supported by narrative regarding performance within the 2019 / 2020 funding year (the first year of delivery post devolution of the AEB to WMCA).
- Further, the WMCA advised that work was being undertaken in liaison with an external partner to produce a three-year evaluation report covering the impact of AEB which would involve learner surveys and interviews with key stakeholders. A draft was expected later in 2021 / 2022.

Audit and Assurance Arrangements

- The Framework suitably refers to compliance and assurance arrangements in addition to the aforementioned performance management and monitoring arrangements.
- Arrangements had been suitably established through engagement of an external provider of audit and assurance services to undertake Funding Compliance reviews of WMCA funded provision.
- The methodology utilised by the external provider appears to align with the ESFA methodology which includes assurance reviews undertaken to assess the ILR returns and associated funding for a particular funding year. Where data errors or anomalies are identified, providers will be asked to explain and, where required, correct ILR data and repay funds.
- An engagement letter was in place covering the scope of Funding Compliance reviews to be undertaken and sample of providers (which included two of the three ITPs within the sample selected for this internal audit) covering the 2019 / 2020 funding year.
- The engagement letter and the draft Funding Compliance review reports (March 2021) for the two sampled ITPs indicated that the scope of review and the resultant content within each report for the 2019 / 2020 funding year clearly aligned with the ESFA's assurance methodology.

Provider Subcontracting

- Testing of sampled providers confirmed that subcontractor declarations had been submitted (as a mandatory requirement of the Framework and contracts / grant agreements) and retained for the 2020 / 2021 funding year.

- A suitable subcontracting declarations register had been maintained and published (accessible via the AEB section of the WMCA website) for all providers. Sampled provider declarations were consistent with the corresponding entries in the register.
- Monitoring of subcontracted delivery was suitably facilitated within the HLRs mechanism (nil return for sampled providers).

Learner Data Collection and Validation

- The Framework supported by the Provider Return Validation Process suitably detailed the data collection and validation arrangements established to validate provider submitted learner data (through the ILR) against learner eligibility criteria within funding rules.
- Data imported from the ESFA Submit Learner Data Portal (mandatory requirement for providers to submit learner data via the Portal which is validated by the ESFA), is then subjected to the WMCA's own data validation by the Productivity and Skills Data Analysis Team.
- The validation processes in place help ensure provider errors in data submissions are referred back to the provider to rectify through subsequent submissions to the ESFA Portal.
- Reports were produced on basis of validation checks of learner data regards what provision should be paid for in a particular period and what provision should not be paid for due to data errors or claims for provision that is not in accordance with funding rules criteria.
- The Validation Process also includes validation checks undertaken by Skills Delivery Officers for delivery monitoring purposes and by Finance for payment purposes.
- Validated provider data as above is also made available to the AEB Team and senior management through the QuickSight database developed and maintained by the Data Analysis Team.
- The above ESFA and WMCA validation processes facilitate both payments and performance monitoring on the basis of validated data to ensure accuracy and completeness as well as confirmation of eligibility against funding rules criteria.

Provider Payment Arrangements

- Suitable arrangements as detailed above had been established for the validation, approval, and processing of payments due to Colleges, Local Authorities, and ITPs.
- Testing for a sample of payments made in the period December 2020 to February 2021 for the three selected ITPs (totalling £1,613,520.95 representing 30% of total ITP payments made in this period) identified that payments had been made in accordance with:
 - Reports detailing payments due per ESFA and WMCA validated learner data regarding eligible delivery.
 - Finance validation (i.e. adjustments relating to changes in delivery levels and ensuring payments to date within contract value limits).
 - Corresponding Payment Briefings detailing payments due.
 - Approval at AEB Payment Group meetings.
- Testing of a sample of profile-based payments for the same period as above for one College and one Local Authority identified that payments had been made in accordance with Payment Briefings, approval at AEB Payment Group meetings and Finance validation. Payments to the

selected College totalled £4,162,751.79 and for the selected Local Authority £1,884,370.91, representing 23% and 10% respectively of total grant payments made in the test period.

- Sampled payments as above suitably reconciled to transactions processed and paid within Business World.
- Testing of total payments made for the same period to all providers totalling £23,657,593.86 (£18,297,569.25 grant payments and £5,360,024.61 ITP payments) identified that amounts reconciled between the total due stated in Payment Briefings, total proposed for payment within Accounts Payable upload spreadsheets, and that recorded as processed payment transactions within Business World.
- Sample testing also confirmed that payments had been made on a timely basis in line with the timescales stated in the Framework.

Acknowledgement

Several employees gave their time and co-operation during this review. We would like to record our thanks to all the individuals concerned.

2. Findings and recommendations

Action is required to avoid exposure to significant risks in achieving objectives
Amber

Legal Services

1. Retention of signed contracts and inclusion of execution dates

Findings:

For the sample selected, two signed grant agreements and two signed contracts relating to the 2019 / 2020 funding year were located by Legal Services. In the remaining instance, a copy of the signed contract with a value of £1,891,553 could not be located by the WMCA within its records. However, upon request to the ITP during the audit, the ITP provided a copy of the signed signature page.

The Public Procurement Regulations 2015 (Part 2, Chapter 4) requires contracting authorities to keep copies of all contracts for at least the duration of the contract where the value exceeds 1,000,000 EUR (£861,630). Whilst evidence was provided by the ITP that the signed contract was in existence, the WMCA had not suitably retained a copy in compliance with the Public Procurement Regulations.

The 2020 / 2021 grant agreements sampled had been retained as signed copies but only one included a deed date of 7 September 2020 which was a month after the start of the funding period. For the three ITPs, the 2019 / 2020 contracts had been extended to cover 2020 / 2021 (permitted by the terms of the contract) but the extension letter notifying the providers had not been signed by the relevant WMCA senior officer and were dated after the start of the funding period. Whilst the deed register may include the execution date, the documents themselves did not include this as complete records in their own right.

Implications:

- Lack of evidence to demonstrate adherence to Public Procurement Regulations may lead to a breach of regulations as well as reputational damage.
- In the absence of signed agreements or clearly stated execution dates within the contract itself, it may be difficult to enforce the terms and conditions of the grant agreement.

Recommendations:

- i. Signed copies of all contracts and grant agreements should be securely and centrally retained as a formal record of the WMCA, and as demonstration of adherence with the Public Procurement Regulations in all cases.
- ii. Copies of signed contracts and grant agreements should be provided immediately after signing to the responsible service area for their operational use and local retention. This should not be a substitute for central retention by Legal Services.
- iii. An exercise should be taken to ensure all contracts and grant agreements for the funding periods 2019 / 2020 and 2020 / 2021 are located and where not held, a copy obtained from the provider. This should be undertaken for all contracts and grant agreements where the value is over the Public Procurement Regulations threshold as a minimum but in all cases as best and consistent practice.
- iv. All contracts and grant agreements should include the date of execution for completeness and demonstration within the document itself that it has been executed prior to the commencement of the funding year and service delivery. Ideally signatures should also be dated.
- v. All extension letters relating to previously executed contracts should be signed by the relevant WMCA senior officer and issued (as in the case for contracts and grant agreements) prior to the commencement of the funding year and service delivery.
- vi. The contract form used for AEB ITPs should be reviewed and revised to ensure that it can facilitate the inclusion of the date upon which the contract is executed as a deed. Ideally all contract forms and grant agreement forms should also facilitate the date of signing by both parties.

Agreed Actions:

The recommendations are agreed. It is acknowledged that there are historic gaps in processes that have led to the department not being able to provide signed copies of contracts in a timely manner. Since the audit, steps have been taken to address the areas of concern identified including:

1. Legal and the AEB client have been working much more closely together, meeting weekly to review contracts. Signed copies of all documents are now scanned and sent to the client. Legal and the AEB client have set up a closed Share-point space to store all signed contracts, both past and current contracts.
2. An exercise has been undertaken to locate all contracts and grant agreements for the funding periods 2019 / 2020 and 2020 / 2021 and copies of these have been placed in the Share-point file. Legal and the AEB client as part of their weekly meetings complete a Contracts tracker which captures all legal instruction and details future pipelines of work. The Acting Lead Solicitor for Productivity, Skills and Public Sector Reform will continue to work with the client develop the tracker to note execution dates and renewal dates.
3. The Acting Lead Solicitor in consultation with the Interim Legal Services Manager will undertake a review of the form of contract to consider the points made around execution and dating of signatures in recommendations iv to vi.
4. An Interim Practice Manager is already in place who is in the process of reviewing the facilities and processes for storage and documentation. The Interim Practice Manager and the Interim Legal Services Manager will then make recommendations for a long-term storage solution for electronic and hard copy documents and put into place a process for storage and documentation. The process will consider where, and by who, the contracts will be held, retention periods and information governance and data security issues, and ensure that the contracts are centrally accessible and that the process is subject to regular spot checks to ensure compliance.

Responsible Officer:

Satish Mistry, Interim Director, Law and Governance
Jayne Middleton, Interim Legal Services Manager

Target Date:

31 December 2021

WMCA Finance**2. Evidencing s151 Officer approval within financial records and audit trail for uploaded transactions****Findings:**

Testing of the transaction records maintained by Finance and Accounts Payable for the sample selected showed that actual evidence of approval by the s151 Officer as granted within AEB Payment Group meetings was not submitted prior to payment being made or retained as part of the WMCA's central financial records and the audit trail.

We understand that for expediency to meet payment deadlines the AEB Accountant submits the Accounts Payable upload spreadsheet via email and states approval was given. Similar emails from the Financial Controller also stated approval was given. However, in both cases this is based on their attendance at the AEB Payment Meeting rather than documentary evidence of approval.

In one case, the deputy s151 Officer had provided email approval although they had not attended the actual Payment Group meeting in person on behalf of the s151 Officer but was understood to have been instead briefed by the Financial Controller who had attended.

All budget managers must provide evidence of approval i.e. via email to Accounts Payable before the upload can be actioned in Business World so as to replicate and comply with the automated workflow built into Business World as standard and requires retention for six years plus one.

However, it is appreciated that minutes of the Payment Group meeting are subsequently produced and awaiting this would delay the payment process which is subject to strict timescales. The Productivity and Skills Finance Business Partner advised that they had retained copies of minutes within their local drive and for confidentiality reasons advised cannot be shared with Accounts Payable.

Implications

- Approval of AEB payments is not clearly evidenced with the WMCA financial records and audit trail to be retained for the required period.
- It may be difficult to demonstrate approval in the event of query or challenge at a later date.

Recommendations:

- i. In all cases and in accordance with standard Accounts Payable spreadsheet upload processes, documentary evidence of approval (including email or minutes) should be provided at the time the spreadsheet is submitted by the service area to Accounts Payable and prior to payments being processed in Business World. Approval evidence must be retained with the uploaded spreadsheet within Accounts Payable as a central financial record and audit trail.
- ii. The Productivity and Skills Finance Business Partner and Financial Controller should clearly evidence responsibility and accountability for confirming approval based on their attendance within their email submissions to Accounts Payable regarding spreadsheets presented for upload.

Agreed Actions:

- i. Documentary evidence of Section 151 Officer approval of payments in the form of the Payment Group minutes will be provided together with the relevant payment files when they are submitted to Accounts Payable with immediate effect. (It is suggested that the minutes of the Payment Group meeting are separated into 2 parts going forward, Part A dealing with the approval of the payments and Part B dealing with provider risks and any sensitive information.)
- ii. The Productivity & Skills Finance Business Partner and the Financial Controller will confirm by email to Accounts Payable that the files submitted are an accurate record of the payments discussed & approved at the Payment Group meeting.

Responsible Officer:

Louise Cowen, Financial Controller
Fahmida Chowdhury, Productivity and Skills Finance Business Partner

Target Date:

31 August 2021

Programme Assurance and Appraisal (Single Assurance Framework)**3. National Local Growth Assurance Framework requirements****Findings:**

The s31 Grant Determination Letter covering devolution of the AEB to the WMCA stated in respect of assurance arrangements that the West Midlands Combined Authority “must have regard to The National Local Growth Assurance framework”, “clarifying what assurances should be in place when administering adult education functions.”

The National Local Growth Assurance Framework states at Annex C: Adult Education Budget Guidelines for Mayoral Combined Authorities what is required to fulfil the above but also states that Combined Authorities are to determine how best to address the guidelines when developing their Local Assurance Framework.

Whilst the WMCA had established a Single Assurance Framework in response to the National Framework, it stated that AEB assurance arrangements would be covered separately.

However, we found that a separate document to meet the requirements of the National Local Growth Assurance Framework at Annex C regarding of a Local Assurance Framework covering AEB was yet to be established.

Implication:

The WMCA may find difficulty in demonstrating compliance with the National Framework requirement to develop an AEB Local Assurance Framework in the absence of an overarching document.

Recommendations:

- i. A suitably detailed and overarching AEB Local Assurance Framework document should be established to meet the requirements of the National Local Growth Assurance Framework.
- ii. The AEB Local Assurance Framework should at all times include reference (and links) to the latest and most up to date AEB Funding Rules, Payment and Performance Management Framework and supporting process documents.

Agreed Actions:

Agreed. WMCA Assurance and Appraisal team will work with AEB to establish the best route for integrating the adult education function into SAF in order to have regard to the National Local Growth Assurance Framework. Any approach must reflect the relatively low risk of the current programme and balance this against the oversight provided through the SAF. The approach will be designed and agreed by 31st December 2021 and integrated with current processes by 30th June 2022. Amendments to the SAF will be made by September 2022 as part of the SAF annual review and approval process.

Responsible Officer: Ian Martin – Investment and Commercial Activities Director Joti Sharma - Head of Programme Assurance & Appraisal	Target Date: 30 September 2022
--	--

Action is advised to enhance risk control or operational efficiency
Green

Productivity and Skills

4. Provider level risk assessments

Findings:

Whilst a risk based approach was evident within both the performance management arrangements operated by the AEB Team and the Financial Due Diligence / Health Assessments operated by Finance, the risk arrangements defined in the Performance Review Framework required review and revision to ensure reflected current and / or developing practice and process.

In addition, there could be clearer integration between the two outcomes to develop a single risk-based view of each provider as well as reflect this more clearly in reporting arrangements. Further this could be enhanced to ensure outcomes integrate with wider risk management at operational, directorate, and strategic levels (as applicable regards the need for escalation).

The above would further support the AEB Payment Group's intention to develop its role regards future reporting and consideration of finance and legal risks in addition to provider delivery risks and issues.

Implications:

Reporting of provide level risk assessment outcomes may not be undertaken collectively.

Recommendations:

- i. Clearer integration of the outcomes of risk assessments within performance management and within financial due diligence activity should be established in order to develop a single risk-based view of each provider and be reflected within performance monitoring and AEB management information and reporting arrangements. This should be further enhanced to ensure outcomes integrate with wider risk management at operational, directorate, and strategic levels (as applicable regards the nature of the risk and need for escalation).
- ii. The AEB Performance Review Framework should be reviewed and revised accordingly to ensure clearly reflects current risk assessment arrangements and supports the above integrated approach between performance management and finance due diligence. The Framework should also reflect how approach integrates with operation, directorate, and strategic level risk management arrangements.

Agreed Actions:

- i. Clearer integration of the outcomes of risk assessments within performance management and within financial due diligence activity will be established in order to develop a single risk-based view of each provider, whilst ensuring the outcomes integrate with WMCA's wider Risk Management Framework. Inclusion of financial due diligence in the provider risk management spreadsheets will be undertaken and will feed into the new AEB Operational Risk Register. Significant financial/delivery risk will be raised in the Payment Group meetings.
- ii. AEB Performance Review Framework is currently under review and will take into account elements raised in the recommendations above and ensure current risk assessment arrangements are clearly reflected.

Responsible Officer:

Iris Both, Senior Delivery Manager Adult Education
Louise Cowen, Financial Controller
Fahmida Chowdhury, Productivity and Skills Finance Business Partner

Target Date:

30 September 2021

WMCA Finance and Productivity and Skills

5. AEB Payment Group administration

Findings:

Action is advised to enhance risk control or operational efficiency
Green

Whilst AEB governance arrangements and specifically in respect of the Payment Group were clearly evident as operational, governance could be further enhanced through establishment of a Terms of Reference detailing (but not limited to) the Group's purpose, authority / delegations and roles and responsibilities.

Also reference to the Group's approval function and delegated authority to the s151 Officer to approve payments through this Group could be clearly stated. Whilst the business of the group was sufficiently documented within minutes, a formal actions and decisions log may more easily facilitate tracking of progress regards actions and implementation of decisions.

Implications:

Governance arrangements may not be fully reflected in the absence of standard administration tools such as terms of reference and logs.

Recommendations:

- i. Suitable terms of reference should be developed for the Payments Group with specific reference to the s151 Officer delegated approval role, as well as (but not limited to) the Group's purpose, membership, meeting frequency and quorum.
- ii. A dedicated action log and decisions log should be developed to support the Payment Group to ensure actions and decisions can be clearly and easily monitored regards progress with implementation.

Agreed Actions: *To be confirmed*

- i. Terms of reference will be developed for the Payments Group with specific reference to the s151 Officer delegated approval role, as well as the Group's purpose, membership, meeting frequency and quorum.
- ii. A dedicated action log and decisions log will be developed to support the Payment Group to ensure actions and decisions can be clearly and easily be monitored.

Responsible Officer:

Louise Cowen, Financial Controller
Fahmida Chowdhury, Productivity and Skills Finance Business Partner
Iris Both, Adult Education Deliver Manager

Target Date:

30 September 2021

Limitations inherent to the internal auditor's work

This report has been prepared solely for the Combined Authority in accordance with the terms and conditions set out in the terms of reference. Internal audit does not accept or assume any liability of duty of care for any other purpose or to any other party. This report should not be disclosed to any third party, quoted, or referred to without prior consent. Internal audit has undertaken this review subject to the limitations outlined below.

Internal control

- Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgement in decision making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Responsibilities of management and auditors

- It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance for the prevention and detection of irregularities and fraud. Internal audit work should not be a substitute for management's responsibilities for the design and operation of these systems.
- Internal audit endeavours to plan audit work so that it has a reasonable expectation of detecting significant control weakness and if detected, will carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.
- Accordingly, these examinations by internal auditors should not be relied upon solely to disclose fraud or other irregularities which may exist.

Stage	Date
Draft issued	13 July 2021
Revised draft issued	27 July 2021
Exit meeting	2 August 2021
Final issued	7 September 2021
ARAC meeting date	29 September 2021



West Midlands Combined Authority

Final Internal Audit Report: General Data Protection Regulations (GDPR) 2021-2022

Report Date: 16 September 2021

Report Distribution: Satish Mistry, Interim Director, Law & Governance
Gurmit Sangha, Data Protection Officer

Laura Shoaf, Interim Chief Executive
Jason Danbury, Strategic Head of Digital and Data

1. Executive summary

Introduction

An audit of the GDPR arrangements for the West Midlands Combined Authority's (WMCA) has been undertaken as part of the approved internal audit plan for 2021-2022.

GDPR was introduced in May 2018 and this review has been undertaken to establish if regulations have been fully embedded within the WMCA. The audit will be based on a compliance review against the Information Commissioners Office (ICO) four steps guidance for Data Controllers. An assessment has been made against each area of the guidance in section two of the report with an assessment and comments made on all the areas irrespective of whether recommendations were made.

Scope and objectives of audit work

Our audit was conducted in conformance with the Public Sector Internal Audit Standards and will consider the following objectives, and the potential risks to the achievement of those objectives:

- To seek assurance that robust management arrangements and controls are in operation for compliance with General Data Protection Regulations (GDPR).

Scope	Potential risks
<p>The scope of the review included the following areas in accordance with the four steps guidance issued by the ICO for Lawfulness, fairness and transparency:</p> <ul style="list-style-type: none">• The lawfulness, fairness and transparency of personal data being processed.• How the data protection rights of data subjects are met.• The accountability and governance policies/procedures and practises in place.• How data security and data breaches are handled.	<ul style="list-style-type: none">• Regulatory action for failure to comply with legislative requirements• Financial penalties• Loss of sensitive information• Reputational damage through adverse reports

Limitations to the scope of our audit

The review was limited to the above scope areas. A separate audit covering cyber security arrangements will be proposed to be considered going forward.

Overall conclusion

Our audit provides **Satisfactory** assurance over the adequacy of the controls reviewed as part of the process to mitigate risks to an acceptable level.

No Assurance	Limited	Satisfactory	Substantial
Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

Key issues identified

We have identified one **amber** issue where improvements could be made, arising from the following:

- The WMCA's Cyber Essentials accreditation of its IT systems expired in November 2020.

In addition, we have raised nine issues classified as **green** which are detailed in section two of this report.

A summary of this report will be presented to the Audit, Risk and Assurance Committee.

Examples of good practice identified

During our work we identified the following examples of good practice in the management of risk, as achieved through the effective design and application of controls:

- The WMCA had an assigned Data Protection Officer (DPO).
- Data held had been captured and recorded in information asset registers (IAR's) within services.
- All new data processing is subject to completion of Data Privacy Impact Assessments (DPIA) which require project managers to consider the lawful basis of processing, which are assessed by the DPO.
- Where consent is required this is obtained as a ground for processing for individuals.
- Where consent is not obtained as reliance on a legitimate interest is used as the lawful basis for processing, the Information Commissions Office's (ICO) three-part test is applied and met in placing reliance.
- The WMCA is registered with the ICO.
- Privacy information had been provided to individuals through privacy notices published on the website and where appropriate bespoke privacy notices provided.

- Data subject rights were found to be recognised and set out in privacy notices published on the website.
- The WMCA has a process to recognise and respond to individuals' requests to access their personal data and data subject rights through the use of privacy notices and the DPO's contact details published on the website.
- A Data Protection Policy is in place which was introduced in June 2018 following GDPR.
- Annual data protection training is mandatory and completed by all staff through the WMCA Learning Pool.
- The WMCA has written terms in contracts with suppliers who act as processors for data requirements in accordance with the Crown Commercial Services Procurement Policy guidance.
- The WMCA Information Assurance Framework sets out the organisation's information risk structure to manage risks.
- Data and information security sit on the Corporate Risk Register.
- An Information Security Group meets on a quarterly basis which is attended by the DPO and managers.
- The DPO works closely with project managers on the importance of considering privacy protection (data protection by design) to integrate data protection into processing activities.
- The DPIA template is completed as part of all projects which result in new data processing.
- A range of data policies are in place including acceptable use, information security and internet and email use policy.

Acknowledgement

Several employees gave their time and co-operation during this review. We would like to record our thanks to all the individuals concerned.

2. Findings and recommendations

Red

Action is imperative to ensure that the objectives for the area under review are met

Amber

Action is required to avoid exposure to significant risks in achieving objectives

Green

Action is advised to enhance risk control or operational efficiency

Information Commissioner's Controllers checklist	WMCA arrangements / controls / procedures in place	Recommendations	Risk Rating	
Step 1 of 4: Lawfulness, fairness, and transparency				
Information you hold				
1	Your business has conducted an information audit to map data flows.	<p>The current process to map data flows began in July 2019 with a request to all Directors and Heads of Departments from the Senior Information Reporting Officer (SIRO) to document the data they hold and how it is processed.</p> <p>Sample testing identified that business areas had completed an Information Asset Register (IAR) which mapped data the business area held and processes. Further, IAR reviews are undertaken by the WMCA Data Protection Officer (DPO). It is acknowledged that reviews had not been undertaken in 2020 due to Covid- 19 but these were scheduled to take place in 2021.</p> <p>A review with the DPO established that a summary register of IAR's was required to act as a central reference point and to maintain oversight of the registers.</p>	<p>A central summary register of IAR's will be maintained to provide oversight of the registers.</p> <p>Responsibility: Gurmit Sangha, Data Protection Officer</p> <p>Target Date: 31 August 2021</p> <p>IAR reviews undertaken by the Data Protection Officer (DPO) will be resumed and completed in 2021 /2022.</p> <p>Responsibility: Gurmit Sangha, Data Protection Officer</p> <p>Target Date: 31 March 2022</p>	<p>Green</p> <p>Green</p>
2	Your business has documented what personal data you hold, where it came from, who you share it with and what you do with it.	This is recorded as part of the IAR process detailed in 1 above and reviewed by the DPO.	N/a	N/a

Information Commissioner's Controllers checklist	WMCA arrangements / controls / procedures in place	Recommendations	Risk Rating	
Lawful basis for processing personal data				
3	Your business has identified your lawful bases for processing and documented them.	<p>The IAR's require Information Asset Owners to consider the lawful bases of processing for all identified data work streams.</p> <p>All new data processing is subject to Data Privacy Impact Assessments (DPIA) which require operational and project managers to consider the lawful basis of processing. Old legacy systems are also recorded on the IARs.</p> <p>All processing is subject to review of DPO to ensure compliance with legislation.</p>	N/a	N/a
Consent				
4	Your business has reviewed how you ask for and record consent.	<p>Consent was found to be required in the WMCA as a ground for processing (i.e. services to individuals using transport systems).</p> <p>Where required the following was found to be compulsory:</p> <ul style="list-style-type: none"> • Clear consent must be obtained from data subjects. • The data subject must "opt-in" to the data processing. WMCA do this by opt-in tick boxes or asking the data subject to sign up (positively subscribe) • Privacy notices are provided to the data subject. • Consent is clearly recorded with functionality to stop processing if consent is withdrawn. 	N/a	N/a
Consent to process children's personal data for online services				
6	If your business relies on consent to offer online services directly to children, you have systems in place to manage it.	N/a. The DPO advised that the WMCA does not process children's personal data for online services.	N/a	N/a

Information Commissioner's Controllers checklist	WMCA arrangements / controls / procedures in place	Recommendations	Risk Rating	
Vital interests				
7	You may be required to process data to protect the vital interests of an individual, your business has clearly documented the circumstances where it will be relevant. Your business documents your justification for relying on this basis and informs individuals where necessary.	N/a. The DPO confirmed that the WMCA have no processing subject to the vital interests ground for processing.	N/a	N/a
Legitimate interests				
8	If you are relying on legitimate interests as the lawful basis for processing, your business has applied the three-part test and can demonstrate you have fully considered and protected individual's rights and interests.	<p>The IAR's require Information Asset Owners to consider the lawful bases of processing for all identified data work streams. (i.e. fulfilling a public interest) The ICO three-part test is applied when using legitimate interests as a ground for processing which consists of:</p> <ol style="list-style-type: none"> 1. Purpose – what is the purpose of processing 2. Necessity – must be able to demonstrate necessity for processing 3. Balancing – the legitimate interest must not override an individual's freedom, interest, rights. <p>Where IAR's state a legitimate interest for processing is undertaken as the grounds for processing the DPO reviews to ensure this is justified and correct.</p> <p>Further, all new data processing is subject to Data Privacy Impact Assessments (DPIA) which require project managers to consider the lawful basis of processing.</p>	N/a	N/a

Information Commissioner's Controllers checklist	WMCA arrangements / controls / procedures in place	Recommendations	Risk Rating	
Data Protection Fee				
9	Your business is currently registered with the Information Commissioner's Office.	A review of the Information Commissioners Office's register established that the WMCA, TfWM, Midlands Connect, and West Midlands Rail Executive are registered with the Information Commissioner's Office.	N/a	N/a
Step 2 of 4: Individuals' rights				
Right to be informed including privacy information				
10	Your business has provided privacy information to individuals.	<p>A review of the WMCA, TfWM, Midlands Connect and West Midlands Rail Executive websites identified privacy notices were provided to data subjects whose personal data is processed.</p> <p>In addition to operating the standard privacy notices, where required, bespoke privacy notices were evidenced as being provided where more detailed/specific information was required.</p>	N/a	N/a
Communicate the processing of children's personal data				
11	If your business offers online services directly to children, you communicate privacy information in a way that a child will understand.	N/a. The DPO confirmed that the WMCA does not offer online services directly to children.	N/a	N/a
Right of access				
12	Your business has a process to recognise and respond to individuals' requests to access their personal data.	<p>All data subject rights were found to be recognised and set out in privacy notices where It is explained that rights can be exercised by contacting:</p> <ul style="list-style-type: none"> • Information.officer@wmca.org.uk • Telephone: Switchboard – 0121 200 2787; Main Contact Centre – 0345 303 67 60 	N/a	N/a

Information Commissioner's Controllers checklist	WMCA arrangements / controls / procedures in place	Recommendations	Risk Rating	
	<ul style="list-style-type: none"> Address: Data Protection Officer, 16 Summer Lane, Birmingham, B19 3SD <p>When responding to a data subject exercising a data subject right, they are provided with an appeal process to any decision made.</p> <p>A review with the DPO established that all data subject rights are managed and responded to by the DPO/Governance Team, with only a few requests received each year (approximately 5). In addition, staff were provided with guidance on subject rights through a fact sheet and mandatory training.</p>			
Right to rectification and data quality				
13	<p>Your business has processes to ensure that the personal data you hold remains accurate and up to date.</p>	<p>A review with the DPO identified that all new data processing is subject to consideration of data accuracy through DPIA's which are subject to sign off by the DPO.</p> <p>Data accuracy was advised to be the responsibility of the teams to manage with Information Leaders appointed in service areas to champion good data practices. However, spot checks by the DPO with teams on data accuracy when reviewing services IAR's would confirm this.</p> <p>It is acknowledged that resources may restrict the extent of such checks as the DPO is solely responsible for Data Protection, all Freedom of Information Requests, all Subject Access Requests, advice / support on data protection matters and information sharing requests from legal and service areas.</p>	<p>The DPO will carry out spot checks on the accuracy of data when carrying out reviews of service IARs.</p> <p>Responsibility: Gurmit Sangha, Data Protection Officer</p> <p>Target Date: On-going</p> <p>To achieve maximum outcomes from limited resources, regular periodic meetings between the DPO and Information Leaders will take place to communicate data practice topics to services areas / leadership teams.</p> <p>Responsibility: Gurmit Sangha, Data Protection Officer</p> <p>Target Date: 31 July 2021</p>	<p>Green</p> <p>Green</p> <p>Green</p>

Information Commissioner's Controllers checklist	WMCA arrangements / controls / procedures in place	Recommendations	Risk Rating	
Right to erasure including retention and disposal				
14	Your business has a process to securely dispose of personal data that is no longer required or where an individual has asked you to erase it.	<p>All new data processing is subject to retention consideration through DPIA's where the process for disposing of data is recorded.</p> <p>Data retention is also subject to the WMCA Retention and Disposal Policy. However, a review of the policy identified that the policy was dated in 2017 and required review.</p>	<p>A review of the 2017 Retention and Disposal Policy will be undertaken.</p> <p>Responsibility: Gurmit Sangha, Data Protection Officer:</p> <p>Target Date: 30 November 2021</p>	Green
Right to restrict processing				
15	Your business has procedures to respond to an individual's request to restrict the processing of their personal data.	<p>All data subject rights requests are managed and responded to by the DPO.</p> <p>Further, privacy notices published on the WMCA website, explained that rights can be exercised by contacting:</p> <ul style="list-style-type: none"> • Information.officer@wmca.org.uk • Telephone: Switchboard – 0121 200 2787; Main Contact Centre – 0345 303 67 60 • Address: Data Protection Officer, 16 Summer Lane, Birmingham, B19 3SD <p>When responding to a data subject exercising a data subject right, details for an appeal process with any decision made is provided.</p> <p>A review with the DPO established that only one request had been received in the last three years.</p>	N/a	N/a
Right to data portability				
16	Your business has processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way,	Data portability is considered on a case by case basis and delivered with the support of WMCA IT Team and the DPO. A review with the DPO established that there had not been many cases to date.	N/a	N/a

Information Commissioner's Controllers checklist	WMCA arrangements / controls / procedures in place	Recommendations	Risk Rating	
	without hindrance to usability.			
	Right to object			
17	<p>Your business has procedures to handle an individual's objection to the processing of their personal data.</p>	<p>All data subject rights are managed and responded to by the DPO/Governance Team.</p> <p>Privacy notices published on the WMCA website explained that rights can be exercised together with an appeal process. The appeal is a three-stage process.</p> <ol style="list-style-type: none"> 1. complaint about processing data or subject access rights dealt with by the DPO 2. if an appeal is received this would go to the Monitoring Officer 3. if still not happy the right to complain to the ICO is available (contact details provided) <p>Staff at WMCA are provided with training on data subject rights through mandatory training.</p>	N/a	N/a
	Rights related to automated decision-making including profiling			
18	<p>Your business has identified whether any of your processing operations constitute automated decision making and have procedures in place to deal with the requirements.</p>	<p>N/a. WMCA is not currently undertaking any automated decision making</p>	N/a	N/a

Information Commissioner's Controllers checklist	WMCA arrangements / controls / procedures in place	Recommendations	Risk Rating	
Step 3 of 4: Accountability and governance				
Accountability				
19	Your business has an appropriate data protection policy.	<p>A Data Protection Policy was implemented in June 2018 following GDPR. The policy is available on the WMCA intranet site.</p> <p>However, a review with the DPO established that a dedicated page on the intranet site where policies, guidance notes and update news articles would provide a more centralised place for data management documents.</p>	<p>Consideration will be given to having a dedicated webpage on the WMCA intranet site to provide a centralised point for employees to access data policies, guidance notes and new updates.</p> <p>The Data Protection Policy will be reviewed to ensure that it is still fit for purpose.</p> <p>Responsibility: Gurmit Sangha, Data Protection Officer</p> <p>Target Date: 31 December 2021</p>	Green
20	Your business monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.	Part of the DPO's roles in reviewing services IAR's is to check for compliance and to take the opportunity to challenge.	N/a	N/a
21	Your business provides data protection awareness training for all staff.	<p>Annual data protection training is mandatory for all staff. The annual training is delivered through WMCA Learning Pool, with employees emailed and managers copied in where training is not completed. Take up is also monitored and reported to HR.</p> <p>Additional ongoing training, guidance, awareness is provided throughout the year where required.</p>	N/a	N/a

Information Commissioner's Controllers checklist	WMCA arrangements / controls / procedures in place	Recommendations	Risk Rating	
Processor contracts				
22	Your business has a written contract with any processors you use.	A review with the DPO established that all new contracts with suppliers that act as data processors are subject to the Crown Commercial Services Procurement Policy guidance clauses. Further, for old contracts an addendum was sent out in 2018.	N/a	N/a
Information risks				
23	Your business manages information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively.	<p>A review with the DPO established that the WMCA Information Assurance Framework sets out the organisation's information risk structure.</p> <p>To manage risk WMCA has in place:</p> <ul style="list-style-type: none"> • An Information Risk Management Policy. • An Information Risk Management Procedure. <p>However, the WMCA has recently reviewed its overall Risk Strategy, and how risk is managed. Information risk will feed into and follow this strategy going forward.</p> <p>Data and information security sits on the Strategic Risk Register.</p> <p>An Information Security Group also meets on a quarterly basis which is attended by managers.</p>	N/a	N/a
Data Protection by Design				
24	Your business has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.	<p>A review with the DPO established that since 2018 the WMCA has implemented a programme of upskilling the workforce on data protection compliance. This has included the concept of considering data protection at the design/planning stage of any process that will result in the processing of personal data.</p> <p>The DPO has worked closely with project managers on the importance of considering privacy protection (data protection by design).</p> <p>Privacy by design is implemented through Data Protection Impact assessments (DPIA)</p>	N/a	N/a

Information Commissioner's Controllers checklist	WMCA arrangements / controls / procedures in place	Recommendations	Risk Rating	
Data Protection Impact Assessments (DPIA)				
25	Your business understands when you must conduct a DPIA and has processes in place to action this.	The DPO supports project teams on DPIA's and provides guidance, training, and awareness on DPIA's. Written guidance to all staff is also available on DPIA's on the WMCA intranet site.	N/a	N/a
26	Your business has a DPIA framework which links to your existing risk management and project management processes.	A review with the DPO established that: <ul style="list-style-type: none"> • The WMCA DPIA template is completed as part of all projects which will result in new data processing. • Where a third party is acting as a Data Processor a Supplier System Risk Assessment template is completed in conjunction with a DPIA. Further this process will link with the new risk strategy.	N/a	N/a
Data Protection Officers (DPO)				
27	Your business has nominated a data protection lead or Data Protection Officer (DPO).	Gurmit Sangha is WMCA Data Protection Lead and DPO and his contact details are included on the WMCA website.	N/a	N/a
Management Responsibility				
28	Decision makers and key people in your business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.	The WMCA Information Assurance Framework sets out the management responsibilities for information assurance.	N/a	N/a

Information Commissioner's Controllers checklist	WMCA arrangements / controls / procedures in place	Recommendations	Risk Rating	
Step 4 of 4: Data security, international transfers, and breaches				
Security policy				
29	<p>Your business has an information security policy supported by appropriate security measures.</p>	<p>A review with the DPO established that the WMCA has the following policies in place:</p> <ul style="list-style-type: none"> • Information Security – Acceptable Use Policy. • Information Security Policy. • Information Security Classification Policy. • Internet & Email Use Policy <p>However, it was identified that the WMCA does not use automated protective marking on their e mails (i.e. Restrict, Protect, Not Protectively Marked)</p> <p>Further, the WMCA's Cyber Essentials accreditation of its IT systems had expired in November 2020 and WMCA ICT is in the process of submitting a renewal application with supporting evidence for assessment by an independent third-party accreditor. We understand that once the application is submitted, there will be a period of time before the WMCA receives its accreditation, after the accreditor has undertaken their assessment subject to any requirements for further clarifications or supporting evidence.</p>	<p>Consideration will be given to introducing automated protective marking on emails.</p> <p>Responsibility: Gurmit Sangha, Data Protection Officer</p> <p>Target Date: 31 December 2021</p> <p>A review of progress with submission of the application for re-accreditation has been undertaken by ICT and the target date for Cyber Essentials submissions is now October 2021. This allows us time to be thorough in our assurance around specific controls in areas of Cyber Essentials that have expanded since our previous submission. Cyber Essentials is not a mandatory requirement for GDPR compliance, but we will proceed with this certification as part of the wider HMG Security Policy Framework mandates.</p> <p>Responsibility: Jason Danbury, Strategic Head for Digital and Data</p> <p>Target Date: 31 October 2021 for submission of application (accreditation date thereafter is subject to the accreditor completing their assessment and any requirement for further supporting evidence)</p>	<p>Green</p> <p>Amber</p>

Information Commissioner's Controllers checklist	WMCA arrangements / controls / procedures in place	Recommendations	Risk Rating	
Breach notification				
30	<p>Your business has effective processes to identify, report, manage and resolve any personal data breaches.</p>	<p>A review with the DPO established that the WMCA has in place:</p> <ul style="list-style-type: none"> • A Security Incident Reporting Policy • A Security Incident Reporting Procedure • Security breaches are reported to SecurityIncidentReporting@wmca.org.uk <p>However, any serious breach would need to be reported to the ICO with 72 hours which would require buy in from Senior Officers with an agreed streamlined procedure to meet the deadline. Senior Officers and Directors would be required to come together at short notice to meet the 72-hour timescale.</p>	<p>An agreed streamlined protocol to meet the ICO reporting deadline for serious breaches will be introduced.</p> <p>Responsibility: Gurmit Sangha, Data Protection Officer</p> <p>Target Date: 31 January 2022</p>	Green
International transfers				
31	<p>Your business ensures an adequate level of protection for any personal data processed by others on your behalf that is transferred outside the European Economic Area.</p>	<p>WMCA will only permit international data transfers (Outside of the UK and EU) only in exceptional circumstances, as it is not the preferred option. Where such transfers are required one of the following are required to be in place:</p> <ul style="list-style-type: none"> • There is in EU adequacy agreement in place. • If the transfer is to the USA, the organisation in the USA is certified to the EU – USA Privacy Shield. • The EU Standard Contractual Clauses for controller to processor are in place 	N/a	N/a

Limitations inherent to the internal auditor's work

This report has been prepared solely for the Combined Authority in accordance with the terms and conditions set out in the terms of reference. Internal audit does not accept or assume any liability of duty of care for any other purpose or to any other party. This report should not be disclosed to any third party, quoted, or referred to without prior consent. Internal audit has undertaken this review subject to the limitations outlined below.

Internal control

- Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgement in decision making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Responsibilities of management and auditors

- It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance for the prevention and detection of irregularities and fraud. Internal audit work should not be a substitute for management's responsibilities for the design and operation of these systems.
- Internal audit endeavours to plan audit work so that it has a reasonable expectation of detecting significant control weakness and if detected, will carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.
- Accordingly, these examinations by internal auditors should not be relied upon solely to disclose fraud or other irregularities which may exist.

Stage	Date
Draft issued	8 July 2021
Revised draft issued	9 August 2021
Final issued	16 September 2021
ARAC meeting date	29 September 2021