INTERNAL AUDIT

Final Assurance Report 2020/21

Creditors

18th December 2020

Overall IA Assurance Opinion:

SUBSTANTIAL

Recommendation Overview:

High Risk	0
Medium Risk	0
Low Risk	4
Notable Practice	0

Review Sponsor:

Emma Beal	Managing Director, West London Waste Authority

Final Report Distribution:

Jay Patel	Finance Director, West London Waste Authority

Ownership of all final Internal Audit assurance reports rests with the relevant Review Sponsor.

1. Introduction

1.1 This risk based Internal Audit (IA) assurance review was requested by management to be undertaken as part of the 2020/21 annual IA plan. **The purpose of this review is to provide assurance to the West London Waste Authority (WLWA) Officers Team and the Audit Committee over the key risks surrounding Creditors:**

- If the administration of creditors is not supported by clear and up to date policies and procedures, there is a risk that payments may be processed inaccurately and in an untimely manner, leading to duplication, errors and inconsistent practices and resulting in financial and legal consequences for the Authority;
- If payments are not made in accordance with authorised purchase orders and goods are not checked upon receipt, there is a risk that the payments could be made that have not been agreed, planned for, or substantiated, leading to potential fraud and unbudgeted expenditure, resulting in financial, operational and reputational consequences for the Authority
- If there is inadequate segregation of duties within payment processes, there is a risk of fraud and collusion that may be undetected, leading to the loss of funds and resulting in financial and reputational damage to the Authority; and
- If the performance of the payments function is not regularly monitored and scrutinised by management, there is a risk that the Authority could make uninformed decisions and incur large creditor balances, resulting in financial, operational and reputational consequences for the Authority.

2. Background

2.1 The creditor's function is overseen by the Finance Director, who is responsible for ensuring that the Authority's payments are processed in accordance with its Financial Regulations. The Authority uses a system called Agresso in order to record transactions on its purchase ledger.

2.2 As specified within its Financial Regulations, the Authority commits to paying all undisputed invoices within 30 days from the day of receipt. Payment terms of less than 28 days can only be agreed with the approval of the Treasurer. It is therefore crucial that this is adhered to, so that the Authority can accurately forecast its cashflow and ensure that there are sufficient funds to meet its current liabilities. Further, the Financial Regulations specify responsibilities for establishing a financial scheme of delegation in respect of payment requests, placing and approving orders, and limits to individual authority.

3. Executive Summary

3.1 Overall, the IA opinion is that we are able to give **SUBSTANTIAL** assurance over the key risks to the achievement of objectives for Creditors. Definitions of the IA assurance levels and IA risk ratings are included at **Appendix C**. An assessment for each area of the scope is highlighted below:

Scope Area	IA Assessment of WLWA
Policies and procedures	**Reasonable Assurance** – The organisation has an overarching Financial Regulations policy in place to specify key procedures and controls within the Authority's financial processes, including the creditors process. A range of supporting procedural guidance was also found to be in place, including for the set up and approval of suppliers, conducting of reconciliations, and preparation, approval and completion of payments.

Scope Area	IA Assessment of WLWA
Policies and procedures (cont'd)	All policies and procedures were found to be readily available to officers involved in the administration and management of the creditors function, where each document could be accessed through the Authority's intranet or via a folder on the shared drive. This therefore promotes good business continuity arrangements and staff awareness of procedures and rules. Although policies and procedures were found to be in place for creditors processes, several documents did not contain adequate version control, or did not contain evidence of regular or recent review. Without sufficient version control, there is a risk of the Authority's policies and procedures failing to reflect current best practice or legislation. As processes and systems update and evolve over time, there is particular need to ensure that procedural guidance remains up to date.
Roles, responsibilities and segregation of duties	**Substantial Assurance –** The Financial Regulations were found to clearly outline and document the Authority's key financial policies and procedures. Job descriptions (JDs) for the 4 primary financial roles also detailed the control responsibilities of each role. The creditors process was found to be governed by a clear segregation of duties for the preparation and approval of supplier accounts and payments, with each supplier account and payment being approved by the Finance Director, after preparation by the Finance Officer. Testing identified a potential control weakness, where Agresso access permissions have been set to allow reviewers of transactions and reconciliations to post accounting transactions on the system. In sample testing, however, there was no evidence of this practice taking place, demonstrating independence. The setting of Agresso permissions in this way does therefore present a potential control weakness, but also promotes business continuity for officers in a small team or organisation. The Agresso system is accessed through a secure remote server, however access controls to Agresso could be improved. Although the system is password-protected, a password policy is not enforced to define the complexity requirements of passwords, potentially resulting in the use of weak user passwords and compromising the integrity of the system.
Supplier setup and amendment	**Substantial Assurance** – Clear and concise procedural guidance was found to be in place for the creation of suppliers in the Agresso system and the information requirements in order to complete this process. A clear list of required information was readily available to ensure only genuine suppliers were used, minimising the risk of fraud. All new supplier accounts are also required to be reviewed and approved by the Finance Director, providing a further layer of scrutiny and demonstrating a robust control environment. Additionally, all contracts currently in effect between suppliers and the Authority are published on the WLWA website, demonstrating transparency to members of the public over the purchasing arrangements in place for the organisation.
Payment processes and authorisation	**Reasonable Assurance** – The Agresso system was found to contain automated controls to prevent officers from entering incorrect or unrecognised account codes or cost centres. Further, data quality and accuracy of transactions records is enhanced by sufficient review and approval of all payments before being finalised within Agresso. This was demonstrated in testing of a sample of transactions, showing each to be uniquely referenced, adequately supported with narrative and supporting evidence, and accurately recorded on Agresso.

Scope Area	IA Assessment of WLWA
Payment processes and authorisation (cont'd)	Accounts payable ledger codes are subject to monthly reconciliation by the Finance Officer. However, testing identified an absence of evidence to show review and approval of recent reconciliations by senior management, although each reconciliation was completed at the beginning of each month. This is likely to be a result of operational difficulties brought by the Covid-19 global pandemic, but controls should be strengthened in this area. Further, whilst the weekly payment runs were slightly disrupted as a result of Covid-19, payment runs were found to be regularly completed during the testing period and with appropriate segregation of duties in place for the raising and approval of the payment runs. Whilst payments were completed consistently, payment run deadlines, or a payment run timetable, had not been published and was not readily available to budget managers in the organisation. Additionally, from a sample of 25 transactions, 93% of payments were found to be processed and completed within 30 days, as per the Authority's Key Performance Indicators (KPI). This strong performance was further strengthened by the Authority's consistent performance against this KPI (see Management information and reporting).
Management information and reporting	**Substantial Assurance** – A suite of KPIs is in place for WLWA to show the organisation's performance against different aspects of service delivery and financial processes. KPI 8 relates directly to financial monitoring, highlighting the average number of days to pay creditors. There was clear and consistent evidence that progress against KPIs is monitored on a regular basis, with updates provided to Members at each Authority meeting. Performance of creditor processes is also highlighted within reports at these quarterly Authority meetings, with narratives to explain any variances to KPIs and whether any remedial action is required. Overall, there is clear oversight of the Authority's expenditure and set thresholds for identifying any lapses in performance of the creditor function.

3.2 The detailed findings and conclusions of our testing which underpin the above IA opinion have been discussed at the exit meeting and are set out in section four of this report. The key IA recommendations raised in respect of the risk and control issues identified are set out in the Management Action Plan included at **Appendix A**. Good practice suggestions and notable practices are set out in **Appendix B** of the report.

4. Detailed Findings and Conclusions

4.1 Policies and procedures

4.1.1 The organisation has an overarching Financial Regulations policy that informs and guides key aspects of the creditors process. Further, the policy was readily available to all WLWA officers through the WLWA intranet. However, the document had not been reviewed or updated since July 2016. As a result, we have raised a recommendation aimed at mitigating the minor risk in this area (refer to **Recommendation 1** in the Management Action Plan at **Appendix B**).

4.1.2 Several guidance documents were in place covering Authority's financial processes. These included WLWA-created documents on reconciliations, approval of suppliers and expenses guidance, as well as third party user guides for the Agresso system.

4.1.3 Of the procedural guidance documents reviewed, 2 policies and 3 procedures were found to not be properly version controlled or subject to regular review. As a result, we have raised a recommendation aimed at mitigating the minor risk in this area (refer to **Recommendation 1** in the Management Action Plan at **Appendix B**).

4.2 Roles and responsibilities and segregation of duties

4.2.1 Roles and responsibilities covering the Authority's financial processes, including the processing and monitoring of payment processes, were clearly documented within policies and procedures. These responsibilities were also captured in the JDs for each of the 4 key financial positions.

4.2.2 Testing identified that there is a clearly defined financial scheme of delegation in place. The scheme clearly defines the delegated authority of key financial roles, including the Managing Director, Clerk and Treasurer as well as outlining an urgency procedure. Budget delegations were also found to be in place for each officer, clearly documenting financial responsibilities and defining budgets and budget limits for the 2020/21 financial year.

4.2.3 During testing, strong controls were found to be in place in relation to the segregation of duties throughout the payments process, including supplier set up and approval, the preparation and approval of payments, and subsequent reconciliations of creditor account codes. From a sample of 25 payment transactions and 5 supplier set ups, it was found that the officer responsible for preparing payment transactions and setting up suppliers on Agresso was different to the officer which approved the transaction or supplier in all 25 transactions and 5 supplier set ups.

4.2.4 The Agresso system was found to be subject to appropriate segregation of duties and access permissions according to each officer's role. Administrative access to the system was granted only to relevant senior officers, where only 3 of the 11 officers with Agresso access having super user access. With Agresso super user access, each of the 3 officers can create and amend user accounts, amend user passwords, and disable user accounts permanently or temporarily.

4.2.5 A potential control weakness was identified in testing, where the reviewer has Agresso permissions to post accounting transactions. However, we found no instances of the reviewer raising a payment during the sample period, demonstrating their independence.

4.2.6 A walkthrough of the Agresso system identified that access to the system is achieved through 2 layers of authentication: entering user credentials on a secure cloud-based server and then entering separate credentials on the Agresso system which is run on the server. A potential control weakness was identified during the 2019/20 IA assurance review of the General Ledger, where the Agresso password policy, including expiry and complexity requirements, had not been clearly specified and documented.

4.2.7 At the time of testing, a password policy was still not being enforced on the Agresso system and, therefore, this issue continues to represent a minor weakness in the integrity of the system. As a result, we have raised a recommendation aimed at mitigating the minor risk in this area (refer to **Recommendation 2** in the Management Action Plan at **Appendix B**).

4.3 Supplier setup and amendment

4.3.1 Clear and concise documented procedure guidance was in place for the creation of suppliers in the Agresso system and the steps required in order to complete this process. A clear list of required information and documentation was readily available to ensure only genuine suppliers were used, minimising the risk of fraud.

4.3.2 All new supplier setups are also required to be reviewed and approved by the Finance Director, providing a further layer of scrutiny and therefore enhancing the control environment.

4.3.3 Testing of a sample of 5 new suppliers found each to have been set up in accordance with procedural guidance. For each new supplier, details had been recorded correctly, adequate supporting documentation was provided, the Finance Director had approved the supplier, and the supplier was included on the approved supplier list. Additionally, all contracts currently in effect between suppliers and the Authority are published on the WLWA website and is readily available to both officers and members of the public.

4.4 Payment processes and authorisation

4.4.1 The creation, monitoring and approval of creditor transactions was found to be supported by a strong control environment. Testing of payment transactions on the Agresso system identified automated controls to prevent officers from entering incorrect or unrecognised account codes or cost centres, mitigating the need for additional journals to reverse transactional errors. Further, all payments are reviewed, approved and signed-off before being finalised in the system, thus ensuring good data quality and accurate record keeping of all transactions.

4.4.2 We tested a sample of 25 creditor transactions from the first 6 months of the 2020/21 financial year and found that all transactions tested were uniquely referenced, adequately supported with narrative, supporting evidence, accurately recorded on the Agresso system and subject to approval by a senior officer.

4.4.3 Testing identified that, each month, accounts payable ledger codes are reconciled by the Finance Officer. Discussion with the Finance Officer found that each reconciliation had been completed each month during the test period, although not reviewed by senior management due to the operational difficulties brought by Covid-19. Crucially, each reconciliation was completed in a timely manner and identified no unreconciled transactions. We have therefore raised a recommendation designed to strengthen controls in this area (refer to **Recommendation 3** in the Management Action Plan at **Appendix B**).

4.4.4 Payment runs were found to be regularly completed during the testing period and with appropriate segregation of duties in place for the creation and approval of the payment runs. Whilst payments were completed consistently, payment run deadlines, or a payment run timetable had not been published and was not readily available to the wider Authority. We have raised a recommendation designed to strengthen controls in this area (refer to **Recommendation 4** in the Management Action Plan at **Appendix B**).

4.4.5 From a sample of 25 transactions, 93% of payments were found to be processed and completed within 30 days, as per the authority's Key Performance Indicators (KPI). This strong performance was further strengthened by the Authority's consistent performance against this KPI (refer to section 4.5 – Management information and reporting).

4.5 Management information and reporting

4.5.1 A suite of KPIs are in place which cover all aspects of the Authority's service, from service delivery to environment and education. A specific KPI is in place to monitor the average number of days to pay creditors, with the target being 30 days. At the time of testing, this KPI was performing at a '**green**' level, showing an average of 8 days to pay creditors, well within the target and the '**red**' threshold of 35 days.

4.5.2 Reports were found to be presented at Authority meetings each quarter which highlight their financial position for that period and for the year to date. This includes narrative to explain any variances in the KPI, highlighting any current trends or areas of concern.

5. Acknowledgement

5.1 Internal Audit would like to formally thank all of the officers contacted during the course of this review for their co-operation and assistance. In particular, the Finance Officer, whose advice and help were gratefully appreciated.

6. Internal Audit Contact Details

This audit was led by: Sam Horton
Internal Auditor

This audit was reviewed by: Nick Cutbill CIA
Principal Internal Auditor

Thank you,

Sarah Hydrie CMIIA, CIA
Head of Internal Audit & Risk Assurance

APPENDIX A

Management Action Plan

No.	Recommendation	Risk	Risk Rating	Risk Response	Management Action to Mitigate Risk	Risk Owner & Implementation date
No High or Medium risk recommendations raised.						

*Please select appropriate Risk Response - for Risk Response definitions refer to **Appendix C**.

APPENDIX B

Good Practice Suggestions & Notable Practices Identified

No.	Observation/ Suggestion	Rationale	Risk Rating
1	Management should ensure all financial policies and procedures are up to date, regularly reviewed and version controlled (para ref 4.1.1 and 4.1.3).	*If financial policies and procedures are not regularly reviewed and properly version controlled there is a risk that information and guidance provided might become obsolete or no longer applicable leading to inaccurate or incorrect practices being carried out resulting in financial, legal, operational and reputational consequences for the Authority.*	LOW ●
2	Management should ensure the Authority's Agresso password policy and procedure are clearly defined and documented, version controlled and widely available to all relevant officers (para ref 4.2.6).	*If the Authority's password policy and procedure is not clearly defined and documented there is a risk that weak or inappropriate passwords could be used leaving key systems and data open to fraudulent activity or theft, resulting in financial and reputational consequences for the Authority.*	LOW ●
3	Management should formalise and publish payment run deadline to ensure all officers across the authority know timeframes when raising payments for suppliers and clients (para ref 4.4.3).	*If payment deadlines are not published and widely accessible to officers there is a risk payments will not be processed in a timely manner, leading to a delay in payments causing the Authority to incur fines and damage relationships with suppliers which has financial and reputational consequences for the Authority.*	LOW ●
4	Management should ensure reconciliations are reviewed and approved by a senior officer, either physically or electronically, once completed by the Finance Officer (para ref 4.4.4).	*If reconciliations are not reviewed and approved by senior officers there is a risk mistakes or inaccuracies are missed or not challenged, affecting the accuracy of the Authority's financial records and subsequent financial position, which has financial, legal and reputational consequences for the Authority.*	LOW ●

APPENDIX C

INTERNAL AUDIT ASSURANCE LEVELS AND DEFINITIONS

Assurance Level	Definition
SUBSTANTIAL	There is a **good level of assurance** over the management of the key risks to the Authority's objectives. The control environment is robust with no major weaknesses in design or operation. There is **positive assurance** that objectives will be achieved.
REASONABLE	There is a **reasonable level of assurance** over the management of the key risks to the Authority's objectives. The control environment is in need of some improvement in either design or operation. There is a misalignment of the level of residual risk to the objectives and the designated risk appetite. There remains **some risk** that objectives will not be achieved.
LIMITED	There is a **limited level of assurance** over the management of the key risks to the Authority's objectives. The control environment has significant weaknesses in either design and/or operation. The level of residual risk to the objectives is not aligned to the relevant risk appetite. There is a **significant risk** that objectives will not be achieved.
NO	There is **no assurance** to be derived from the management of key risks to the Authority's objectives. There is an absence of several key elements of the control environment in design and/or operation. There are extensive improvements to be made. There is a substantial variance between the risk appetite and the residual risk to objectives. There is a **high risk** that objectives will not be achieved.

1. **Control Environment:** The control environment comprises the systems of governance, risk management and internal control. The key elements of the control environment include:
   - establishing and monitoring the achievement of the Authority's objectives;
   - the facilitation of policy and decision-making;
   - ensuring compliance with established policies, procedures, laws and regulations – including how risk management is embedded in the activity of the Authority, how leadership is given to the risk management process, and how staff are trained or equipped to manage risk in a way appropriate to their authority and duties;
   - ensuring the economical, effective and efficient use of resources, and for securing continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness;
   - the financial management of the Authority and the reporting of financial management; and
   - the performance management of the Authority and the reporting of performance management.

2. **Risk Appetite:** The amount of risk that the Authority is prepared to accept, tolerate, or be exposed to at any point in time.

3. **Residual Risk:** The risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk.

APPENDIX C (cont'd)

RISK RESPONSE DEFINITIONS

Risk Response	Definition
TREAT	The probability and / or impact of the risk are reduced to an acceptable level through the proposal of positive management action.
TOLERATE	The risk is accepted by management and no further action is proposed.
TRANSFER	Moving the impact and responsibility (but not the accountability) of the risk to a third party.
TERMINATE	The activity / project from which the risk originates from are no longer undertaken.

INTERNAL AUDIT RECOMMENDATION RISK RATINGS AND DEFINITIONS

Risk	Definition
HIGH ●	The recommendation relates to **a significant threat** or opportunity that impacts the Authority's corporate objectives. The action required is to mitigate a substantial risk to the Authority. In particular it has an impact on the Authority's reputation, statutory compliance, finances or key corporate objectives. **The risk requires senior management attention**.
MEDIUM ●	The recommendation relates to **a potentially significant threat** or opportunity that impacts on either corporate or operational objectives. The action required is to mitigate a moderate level of risk to the Authority. In particular an adverse impact on the Department's reputation, adherence to Authority policy, the departmental budget or service plan objectives. **The risk requires management attention**.
LOW ●	The recommendation relates to **a minor threat or opportunity** that impacts on operational objectives. The action required is to mitigate a minor risk to the Authority as a whole. This may be compliance with best practice or minimal impacts on the Service's reputation, adherence to local procedures, local budget or Section objectives. **The risk may be tolerable in the medium term**.
NOTABLE PRACTICE ●	The activity **reflects current best management practice** or is an innovative response to the management of risk within the Authority. **The practice should be shared with others**.