



INTERNAL AUDIT

Final Assurance Report 2019/20

General Ledger

20th March 2020

Overall IA Assurance Opinion:

SUBSTANTIAL

Recommendation Overview:

High Risk	0
Medium Risk	0
Low Risk	3
Notable Practice	0

Review Sponsor:

Emma Beal

Managing Director, West London Waste Authority

Final Report Distribution:

Jay Patel

Head of Finance and Performance, 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 2018/19 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 General Ledger:**
- If General Ledger processes are not sufficiently defined and documented within procedural guidance, there could be a lack of accountability and clarity over working practices, leading to transactions failing to be recorded accurately and in a timely manner, resulting in uninformed decision-making and financial loss to the Authority;
 - If staff are not appropriately trained, there is a lack of contingency cover and potentially insufficient segregation of duties, which could result in transactions not being recorded in the General Ledger on time or accurately and funds not being accounted for, leading to financial loss, legal implications, regulatory scrutiny and operational issues;
 - If transactions are not processed in an effective, accurate or timely manner, there is an increased likelihood that the General Ledger will be inaccurate and incorrectly inform management of the current financial position of the Authority, potentially leading to significant financial loss and reputational damage to the Authority; and
 - If the General Ledger is not regularly monitored or reported, senior management could have an unclear understanding of the Authority's financial position and funds may not be accounted for, resulting in uninformed decision-making, potential non-compliance with financial codes and misappropriation of funds.

2. Background

- 2.1 A General Ledger represents the record-keeping system for a company's financial data with debit and credit account records validated by a trial balance. The General Ledger provides a record of each financial transaction that takes place during the life of an organisation.
- 2.2 The General Ledger holds account information that is needed to prepare the company's financial statements. WLWA's transaction and financial data is segregated by type into four key elements:
- Treasury;
 - Banking;
 - Accounts Receivable; and
 - Accounts Payable.
- Responsibility for processing and reconciling transactions within each of these rests with the Finance Officer, with oversight from the Head of Finance and Performance.
- 2.3 WLWA utilises the Unit4 software application Agresso as its financial management system, with external administration being provided by Unit4's client support team. Its reporting functionality enables up-to-date and relevant financial information to be drawn from the system, which can be used as a basis to conduct management of the General Ledger.

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 General Ledger. 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	<p>Reasonable Assurance – The organisation has 2 overarching financial policies that inform and guide key aspects of the financial process, including the General Ledger: The Financial Regulations and the Contract and Procurement Rules. Further, procedural guidance was found to be in place covering key aspects, including the set up and approval of suppliers, conducting of control account reconciliations, and identifying and rectifying payroll errors.</p> <p>Additionally, all policies and procedures were found to be readily available and easily accessible to relevant WLWA officers, either through the Authority's intranet or within electronic shared folders.</p> <p>Whilst testing identified policies and procedures were in place for key financial processes, several documents were found to not be version controlled or have not been regularly or recently reviewed. The use of proper version control is important in ensuring that policies and procedures accurately reflect current expected practices, regulations and, where applicable, legislation.</p>
Roles and responsibilities	<p>Substantial Assurance – Financial roles and responsibilities were clearly outlined and documented in the key financial policies and procedures in place at WLWA, primarily within the Authority's Financial Regulations. Further detail was provided in the job descriptions (JDs) for the 4 main financial roles within the Authority. However, of the 4 JDs reviewed, it was found that whilst all were version controlled, 2 JDs had not been reviewed since February 2015 and March 2017. Further, all 4 JDs described the principal location of each role as the Authority's former address (Hounslow Civic Centre).</p> <p>Strong controls were found to be in place for General Ledger processes, particularly where duties have been segregated in the updating and approving of General Ledger journals and reconciliations of control accounts.</p> <p>A potential control weakness was identified in testing, where the reviewers of journals and reconciliations have Agresso permissions to post accounting transactions on the system. However, we found no instances of the reviewer posting General Ledger transactions during the sample period, demonstrating their independence. Finance staff also keep a register of General Ledger journals that shows each journal's preparer and approver, ensuring that duties are separated and monitored appropriately. This is particularly important in a small team with relatively few officers.</p> <p>Further, controls were found to be in place for accessing the Agresso system through a secure remote server, although the Authority's Agresso password policy and process had not been documented, resulting in a potential minor weakness in the integrity of the system.</p>
Transactions, data quality and year-end	<p>Substantial Assurance – A strong control environment was found to be in place surrounding the creation, monitoring and approval of journal entries and transactions. Automated controls were found to be in place, preventing officers from entering incorrect or unrecognised account codes or cost centres. Further, all journal entries and transactions are reviewed, approved and signed-off before being finalised in the system, thus ensuring good data quality and accurate record keeping of all transactions and journal entries.</p>

Scope Area	IA Assessment of WLWA
Transactions, data quality and year-end (cont'd)	<p>Additionally, we tested a sample of 15 transactions from the past 10 months and found all transactions tested were uniquely referenced, adequately supported with narrative and supporting evidence and accurately recorded on the Agresso system.</p> <p>Each of the Authority's control accounts is subject to monthly reconciliation which, as per General Ledger journal controls, were governed by an appropriate segregation of duties. The number of unreconciled transactions across the sample of reconciliations tested was minimal and there was evidence that each was reviewed swiftly.</p> <p>Clear, documented guidance was found to be in place for the year-end and account closing processes. This procedural guidance was supported and reinforced with the production of a year-end timetable. This timetable clearly documented the roles and responsibilities for each finance officer at each key stage of the process.</p> <p>Further, the timetable for the 2019/20 year-end process was found to be in the process of being drafted at the time of testing, highlighting continuity in closedown processes and the key roles and responsibilities within it.</p>
Management information	<p>Substantial Assurance – A suite of Key Performance Indicators (KPI) is in place for WLWA covering all aspects of the Authority's service, from service delivery to environment and education. KPIs 5 and 6 relate directly to financial monitoring, highlighting specifically trade debt and average days to pay creditors. Clear evidence was provided to show that progress against KPIs is monitored consistently, with the master KPI spreadsheet updated on a monthly basis and presented at Joint Committee meetings.</p> <p>Further, reports are presented at Joint Committee meetings each quarter to highlight the Authority's financial position for that period and for the year to date. This includes narrative to explain any variances between budgets and actual expenditure, highlighting any current trends or areas of concern.</p>

- 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 Authority has 2 overarching financial policies in place: Financial Regulations and the Contract and Procurement Rules. Both policies set out the overall standards for financial processes within WLWA and were readily available to all WLWA officers through the WLWA intranet. However, the Contract and Procurement Rules are not subject to version control. Additionally, neither document had 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 place covering Authority's financial processes. These included WLWA-created documents on reconciliations, approval of suppliers, upload of payroll and the year-end process, as well as third party user guides for the Agresso system.

4.1.3 Whilst there is no specific documented guidance in place for General Ledger processes such as journals, although given the size of the organisation and the procedural guidance already in place, the creation of procedural guidance specific to the General Ledger is not essential.

4.1.4 Of the procedural guidance documents reviewed, several documents 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

4.2.1 The roles and responsibilities for the Authority's financial processes, including the processing and monitoring of General Ledger transactions, were clearly documented within policies and procedures. These responsibilities were also captured in the JDs for each of the 4 key financial positions. Whilst all were version controlled, 2 JDs had not been reviewed since February 2015 and March 2017. Further, all 4 JDs described the principal location of each role as the Authority's former address, Hounslow Civic Centre. 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**).

4.2.2 WLWA have a clearly defined financial scheme of delegation in place. This scheme clearly defines the delegated authority of key financial figures, including the Managing Director, Clerk and Treasurer as well as outlining an urgency procedure. Further, budget delegations for each officer with financial responsibilities are clearly documented, defining their respective budgets and budget limits for the 2019/20 financial year.

4.2.3 Strong controls were found to be in place in relation to the segregation of duties throughout the end-to-end financial process, including the preparation and approval of General Ledger journals and control account reconciliations. From a sample of 15 journal entries, it was found a different officer entered and prepared the journal entry while a different officer approved the journal entry in all 15 samples. The remaining 2 entries sampled were journal reversals and therefore these journals did not require secondary approval.

4.2.4 Further, it was found there was appropriate segregation of duties and levels of access to the Agresso system. During testing it was found administrative access to the system was granted to relevant senior officers, with only 3 of the 10 officers with system access being granted super user access. These 3 super users were able to create and amend user accounts, renew and resets passwords as well as temporarily and permanently disable user accounts within the Agresso system.

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 posting General Ledger transactions during the sample period, demonstrating their independence. Further, a log was found to be in use to record the preparing and reviewing officers for each journal transaction posted on Agresso.

4.2.6 Access to the Agresso system is achieved through 2 layers of authentication: entering user credentials on a secure cloud-based server and then entering separate credentials on the actual Agresso system which is run on the server. Despite this, the Authority's Agresso password policy, including expiry and complexity requirements, had not been clearly defined and documented. There is therefore 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 3** in the Management Action Plan at **Appendix B**).

4.3 Transactions, data quality and year-end

- 4.3.1 A strong control environment was in place for the creation and approval of journal entries. Automated controls within Agresso prevent officers from creating journal entries under unrecognised account codes or for legitimate journal entries to be entered under Cost Centres that have not been pre-approved and held within the system.
- 4.3.2 Further, good data quality is ensured as all Journal entries are reviewed and approved by a senior officer before being finalised. Each approval is signed by the senior officer and securely stored on site at the Authority.
- 4.3.3 To provide further assurance over the control environment we selected a sample of 15 transactions from the past 10 months to ensure transaction were consistently recorded and accurately. Of the sample of 15 transactions, we found all transactions were uniquely referenced, adequately supported with narrative and supporting evidence and accurately recorded on the Agresso system.
- 4.3.4 Clear, documented guidance was found to be in place for the year-end and account closing processes, mapping out the full process and providing detailed instructions for each stage. This guidance was supported and reinforced by the production and completion of a year-end timetable. This timetable defined the roles and responsibilities of each key officer at every stage of the process, as well as monitoring and tracking the completion of each process stage.
- 4.3.5 During testing, it was identified that the General Ledger was supported by an electronic BACS interface, used for importing BACS payment data automatically into the Agresso system. A strong control environment was found to be in place around this system, where BACS payment runs are subject to monthly approval by the Head of Finance and Performance after being completed by the Finance Officer. Further controls are in place where such BACS payments form part of monthly Accounts Payable and Bank reconciliations, where discrepancies and imbalances would be identified.

4.4 Management information

- 4.4.1 A suite of Key Performance Indicators (KPI) is in place for WLWA covering all aspects of the Authority's service, from service delivery to environment and education. KPIs 5 and 6 relate directly to financial monitoring, highlighting specifically trade debt and average days to pay creditors. These KPIs are monitored and updated monthly providing senior management of the Authority's performance in these key financial areas. Further, clear evidence was provided to show that progress against KPIs is monitored consistently, with the master KPI spreadsheet updated on a monthly basis and presented at Joint Committee meetings.
- 4.4.2 Joint Committee meetings are held quarterly and are attended by senior WLWA management and Members from constituent boroughs. These meetings provide high-level overview of the Authority's performance, both operational and financial, and provide opportunity for financial performance and governance to be scrutinised. The Committee also approves and signs-off the annual accounts and end-of-year financial reports, ensuring there is oversight and understanding of the Authority's financial position from the highest level.

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 Senior Accountant and 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
Senior 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).	<i>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 to current practices, potentially leading to inaccurate or incorrect practices being carried out and insufficient segregations of duties, affecting the accuracy of the Authority's financial records and subsequent financial position.</i>	LOW ●
2	Management should ensure all job descriptions are up to date, regularly reviewed and version controlled. (para ref 4.2.1).	<i>If job descriptions do not hold accurate and up to date information there is a risk job roles will be inaccurately or poorly defined, potentially leading to a lack of understanding of officer responsibilities causing key tasks to lack ownership and being completed late or not completed at all, resulting in financial and operational consequences for the Authority.</i>	LOW ●
3	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).	<i>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.</i>	LOW ●

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.