

**West
Waste**

INTERNAL AUDIT

Final Assurance Report 2019/20

Business Continuity

6th January 2020

Overall IA Assurance Opinion:

REASONABLE

Recommendation Overview:

High Risk	0
Medium Risk	2
Low Risk	0
Notable Practice	1

Review Sponsor:

Emma Beal

Managing Director, West London Waste Authority

Final Report Distribution:

Jay Patel

Head of Finance and Performance, West London Waste Authority

Tom Beagan

Senior Contracts Manager, 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 2019/20 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 Business Continuity:**
- If there is no effective strategy in place for business continuity planning, the organisation may not identify risks to service continuity and allocate sufficient resources to bringing back its operations swiftly after a significant event, causing significant business interruption and resulting in reputational, financial, operational and legal consequences;
 - If there is insufficient ownership and communication of the business continuity planning and execution processes, there is a risk that staff and contractors may be unaware of the procedure to follow in the event of a system or service outage, causing significant downtime for the business and potential risks to staff, and resulting in reputational, financial, operational and legal consequences;
 - Without a clear system of reporting and monitoring in place for business continuity planning, there is a risk that critical services or processes may not be reviewed and covered by a business continuity plan, leading to potential service disruption and risks to staff and service users, resulting in reputational, financial, operational and legal consequences; and
 - If business continuity plans are not regularly tested and reviewed, there is the possibility that plans may not be executed correctly or at all due to a lack of ownership or understanding of the process, causing operations to fail which should be brought back swiftly following system outage or service disruption, leading to operational and financial consequences.

2. Background

- 2.1 Effective business continuity is implemented by creating a comprehensive plan of action for the organisation and its services, which enables all business critical components to be accessible to relevant employees in the event of a major disaster or system outage. It is important that organisations consider their key services, processes, customers and systems and tailor their plans to each of these areas, mitigating the risk posed to the organisation's performance by a significant and unforeseen event.
- 2.2 At present, WLWA does not have an organisation wide Business Continuity Plan outlining a process of systems to deal with potential threats to the company and therefore enabling operations to keep going after a potential disaster. Plans are kept at service level and are tailored to the risks of each team and the processes under their remit. These enable any gaps in service continuity to be identified, highlighting any weaknesses and, as a result, provide assurance that the organisation can still run effectively should the worst-case scenario occur.

3. Executive Summary

- 3.1 Overall, the IA opinion is that we are able to give **REASONABLE** assurance over the key risks to the achievement of objectives for Business Continuity. 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, Procedures and Strategies	<p>Limited Assurance – The Authority consists of 4 key service areas: Resources, Operations, Contracts and Waste Minimisation. There is no overarching policy or guidance governing business continuity planning for these areas. However, business continuity arrangements are in place for key service areas, specifically those that could be seen as more operationally critical such as Resources, Contracts and Operations. The absence of an overarching policy and accompanying procedures has therefore not resulted in a significant weakness in the overall control environment and the residual risk is not high.</p> <p>Despite the residual risk not being significant, the Authority would benefit from a central, overarching policy or template to set a standard across the organisation for business continuity planning. Areas could include officer responsibilities, review and testing schedules for plans, resource requirements, risk assessment of services or functions, and lines of communication. Procedural guidance would also assist officers with the production and review of business continuity arrangements, but such guidance could be incorporated into an overarching template.</p>
Roles and Responsibilities	<p>Reasonable Assurance – Responsibilities for business continuity planning across the organisation are contained within job descriptions, either as explicit duties or within a wider context of responsibilities. It is the responsibility of management of each of the 4 key service areas to ensure proper governance and planning arrangements are in place for their respective area. At a corporate level, the Managing Director is assigned with overall responsibility for ensuring that the organisation is monitoring and assessing its business continuity needs and arrangements.</p> <p>Within the business continuity documents in place for key service areas, key contacts have been specified for critical areas that are required to be maintained during an unforeseen event. In the business continuity plan (BCP) for Finance, an officer is assigned responsibility for each critical task, so that contingency arrangements can be managed in a timely manner. Tasks are not split in this way for the Operations business continuity plans as these are more ad-hoc arrangements.</p> <p>Lines of communication are generally in place in the business continuity documents provided, accounting for operational staff and the need to keep chief officers informed of the outcomes following an event. However, there is no formalised reporting line in place specifying who should be informed and consulted during the planning and execution phases of business continuity plans.</p>
Reporting and Monitoring	<p>Reasonable Assurance – The creation and implementation of business continuity plans is not formally monitored across the organisation at a senior management level. Instead, it is the responsibility of service management to create, implement and report back.</p> <p>Higher-level oversight to scrutinise and monitor the plans could be improved, although the service areas that are essential to the daily operations of the organisation are covered by contingency planning arrangements and the results of these are fed back to key stakeholders, including Chief Officers and contractors.</p>

Scope Area	IA Assessment of WLWA
<i>(Reporting and Monitoring – cont'd)</i>	<p><i>(Reporting and Monitoring – cont'd)</i></p> <p>It was noted during testing that key operations utilise messaging services to keep staff, contractors and other officers up to date in the event of an incident. This enables early awareness of issues to be raised and business continuity measures to be implemented at short notice and even out of hours.</p> <p>Risks to business continuity are assessed at a strategic and operational level, being captured within risk registers. There is also a clear link between the risks that have been assessed and the plans that are in place for key service areas, sites, and contractors.</p> <p>For the documents that are in place, each contains contact information for contractors and staff who would need to be consulted to keep the critical areas of the business running during an unforeseen event.</p>
Plan Testing and Training	<p>Reasonable Assurance – There is no set standard or requirement in place at the organisation for the frequency of testing or review of business continuity plans. This aspect is kept at an operational level and is specified in the formally documented business continuity plan for one of the service areas.</p> <p>A testing schedule is not consistently implemented across the organisation to ensure that information contained within such plans remains accurate and current. Formal testing of plans should generally consist of checking that phone numbers for key contacts are correct and working, that backup offices or sites can be utilised at short notice and that the resources required to implement plans have been accurately captured.</p> <p>We saw evidence, which shows that the documents provided for key service areas has been reviewed in the last 12 months. Further, one of the plans identified that there was no testing required, where the tasks involved with ensuring continuity are conducted using cloud-based servers, which are used on a daily basis and can be accessed on any internet-enabled device. Testing has occurred on a regular basis for operational sites, where incidents such as fires occur frequently. There is also evidence that the results of such incidents are fed back to key stakeholders for future learning.</p> <p>Overall, the business continuity documents in place showed consideration of staffing and resource requirements and alternative sites or offices to continue operating at short notice, although there were some disparities in the way that continuity arrangements have been documented between service areas.</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, Procedures and Strategies

- 4.1.1 Prior to testing, we sought to identify whether the Authority has in place any overarching documents to set the requirements and expectations for business continuity planning.
- 4.1.2 It was found that there is no set policy or overarching document that covers business continuity, and, instead, managers of the 4 service areas are responsible for the creation and implementation of plans. Whilst there is no central standard in place, we found that service areas that are critical to the daily functioning of the organisation (i.e. Resources, Contracts and Operations) were covered by business continuity plans, demonstrating that there is no significant residual risk due to gaps in the control environment.
- 4.1.3 The Resources team have in place a formally documented business continuity plan, which adequately captures the risks to its processes and the recovery processes to mitigate these. Due to the nature of this document, it could be used as a template for the remaining 3 service areas to conform to. As a result, we have raised a recommendation aimed at mitigating the risk in this area (refer to **Recommendation 1** in the Management Action Plan at **Appendix A**).
- 4.1.4 Following a review of the business continuity planning documents we found there is no specific guidance in place to assist management in creating and executing business continuity plans within their respective areas. In line with para. 4.1.3, the plan that was provided for the Resources service could be enhanced and used as a template to guide managers within the remaining 3 service areas. Any guidance should direct service management to consider the following aspects:
- Responsibilities for creating, approving and reviewing the plan;
 - A risk assessment of functions;
 - The continuity processes involved;
 - Staff and resource needs to execute the plan;
 - Communication and storage of plans;
 - Reporting lines between operational staff, service management and senior management; and
 - A schedule for testing components within the plan for relevance and accuracy.

As a result, the suggestions listed above form part of the recommendation raised in para 4.1.3 (refer to **Recommendation 1** in the Management Action Plan at **Appendix A**).

4.2 Roles and Responsibilities

- 4.2.1 Testing identified that responsibilities for business continuity planning are held at an operational level, with service management being responsible for ensuring that continuity arrangements have been considered for their respective areas. These responsibilities were found to be contained within job descriptions for 3 out of 4 service managers, either explicitly referenced or implied as part of their wider responsibilities. For the services that are considered as more critical to the daily functioning of the organisation, responsibilities were shown to be contained within the job descriptions for those service managers.
- 4.2.2 The BCP for the Resources service was found to contain key lines of communication, incorporating officers at an operational level, as well as identifying the need to keep Chief Officers informed should initiation of the plan be required.

4.2.3 The continuity documents for the Operations service contain specific contact information for operational staff at the constituent Borough Councils and the various waste sites, distinguishing first and second points of contact at each, where applicable. This information was distributed as part of contingency planning for the Christmas 2018 period, with plans to keep this updated for other peak periods such as Easter, but has not been formalised as part of a specific or organisation-wide BCP. As a result, we have raised a recommendation aimed at mitigating the risk in this area (refer to **Recommendation 1** in the Management Action Plan at **Appendix A**).

4.2.4 Review of the business continuity arrangements for the Resources and Operations services found that decision-making responsibilities were specified within them. This includes the officer responsible for each continuity/ recovery process within the Finance BCP and the duty officers over the peak season for Operations. Although these arrangements are extensive, the Operations plans do not formally document criteria for initiating backup waste facilities, or when to contact relevant personnel during peak periods. As a result, we have raised a recommendation aimed at mitigating the risk in this area (refer to **Recommendation 1** in the Management Action Plan at **Appendix A**).

4.3 Reporting and Monitoring

4.3.1 Review of meeting minutes from WLWA Officers and Management meetings found that business continuity arrangements had not been discussed from a planning perspective. Instead, evidence was provided to show that the outcomes of incidents affecting business continuity had been reported to Chief Officers and shared amongst key stakeholders, including contractors, officers from constituent Borough Councils, and members of the public.

4.3.2 Whilst it would not be necessary to consider business continuity at every Officer or Management meeting, there should be controls in place to provide a high level of oversight and monitoring to ensure appropriate plans are in place across the organisation and that each has been reviewed and tested, at least annually. As a result, we have raised a recommendation aimed at mitigating the risk in this area (refer to **Recommendation 2** in the Management Action Plan at **Appendix A**).

4.3.3 Our testing of documentation found that risk assessment occurs at a strategic and operational level in order to identify which services, facilities and processes require business continuity plans. At an operational level, the Resources BCP has formally assessed and documented its critical services, putting in place mitigating actions accordingly. For Contracts and Operations, risks have been captured in a risk register with each risk having corresponding management actions. From these actions, operational BCPs have been put in place, such as implementing alternative waste sites in the event that a site becomes unavailable.

4.3.4 In the Resources BCP, there is a section for 'Key Contacts', which holds a comprehensive list of operational staff and contractors, including their contact details, in the event that they should be consulted during an unforeseen event. Review of the document properties found it to have been created within the last 12 months, demonstrating that the details have been recently reviewed.

4.3.5 For Operations, contact details are kept on a master spreadsheet and evidence showed its distribution to relevant contacts to ensure continuity of services over peak periods, such as Christmas 2018, including plans to keep this updated for Christmas 2019 and other peak periods. Further, Operations hold a list of alternative waste facilities that can be utilised in the event of a site not being available. A notable practice was identified where WhatsApp groups are used by officers, at different waste sites, to promote information sharing and raising early awareness of potential issues. We consider this to be good practice (refer to **Notable Practice 3** in the Management Action Plan at **Appendix B**).

4.4 Plan Testing and Training

- 4.4.1 In the Finance BCP, testing arrangements are included as a dedicated section for each of the critical functions and recovery processes. 4 critical functions had been identified in total: IT, office space, supplier payments and finance staffing. Each of these critical areas has a specified testing arrangement. Due to the implementation of working from cloud-based servers, the risks associated with the continuity processes for each areas are mitigated and testing of these functions is therefore not required.
- 4.4.2 As referenced in paras 4.2.3 and 4.3.5, the business continuity arrangements in place for the Operations service includes a listing of contacts at each of the key operational sites, constituent Borough Councils and other key contractors, as well as a listing of alternative waste facilities. As well as these documented contacts and sites (created in January and April 2019 respectively), there is no formal provision for the testing and review of the arrangements.
- 4.4.3 We found that plans are tested on an ad-hoc basis but due to the frequency of incidents such as fires, etc. testing is actually occurring on a regular basis. It would be beneficial to implement a more formal schedule of testing for the documents and plans held across the organisation. Testing should include a review of the list of personnel and their contact details to ensure they are correct, alongside a physical check that phone numbers or email addresses are working. As a result, we have raised a recommendation aimed at mitigating the risk in this area (refer to **Recommendation 1** in the Management Action Plan at **Appendix A**).

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 Head of Finance and Performance and the Senior Contracts Manager, whose advice and help were gratefully appreciated.

6. Internal Audit Contact Details

This audit was led by: Nick Cutbill
Senior Internal Auditor

Audit support was provided by: Sonal Patel
Internal Auditor

This audit was reviewed by: Jenia Islentsyeva FCCA, CISA
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
1	<p>Management should ensure there is a central policy/ template in place, which sets the required standard for documenting and reviewing BCPs for each key service area which include:</p> <ul style="list-style-type: none"> • Responsibilities for creating, approving and reviewing plans; • A risk assessment of functions; • Continuity processes and criteria for initiation; • Staff and resource needs to execute the plan, including out of hours arrangements; • Communication and storage of plans; • Reporting lines across the organisation and stakeholders; and • A schedule for testing components of the plan. <p>(para refs. 4.1.3, 4.1.4, 4.2.3, 4.2.4 and 4.4.3).</p>	<p><i>If there is no standard practice in place for the creation, review and approval of business continuity plans, there is a risk that plans may not be created and monitored consistently for critical service areas, resulting in a loss of service functionality during an unforeseen event causing operational, financial and reputational consequences.</i></p>	<p>MEDIUM</p> <p>●</p>	<p>TREAT</p>	<p>Management will implement a policy or template for the documentation and review of business continuity arrangements, as per the recommendation.</p>	<p><i>Head of Finance</i></p> <p style="text-align: center;"><i>Jay Patel</i></p> <p style="text-align: right;"><i>31st March 2020</i></p>

*Please select appropriate Risk Response - for Risk Response definitions refer to [Appendix C](#).

APPENDIX A (cont'd)

Management Action Plan

No.	Recommendation	Risk	Risk Rating	Risk Response	Management Action to Mitigate Risk	Risk Owner & Implementation date
2	Management should ensure that there is sufficient high-level oversight and monitoring of business continuity planning, ensuring that service management have implemented sufficient business continuity plans and that these have been regularly reviewed for accuracy and relevance (para ref 4.3.2).	<i>If there is insufficient oversight of business continuity planning, there is a risk that critical services will not be assessed and planned for, leading to a loss of functionality during an unforeseen event and resulting in operational, financial and reputational consequences.</i>	MEDIUM 	TREAT	Management will implement annual monitoring, review and oversight of business continuity planning.	<i>Head of Finance</i> <i>Jay Patel</i> <i>31st March 2020</i>

*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
3	The use of WhatsApp groups was found to be an innovative way of maintaining contact with key stakeholders and communicating issues at waste sites at an early stage, including outside of working hours, in preparation for continuity arrangements to be initiated.	<i>The activity reflects current good practice or is an innovative response to the management of risk which has been shared with others.</i>	NOTABLE PRACTICE ●

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.