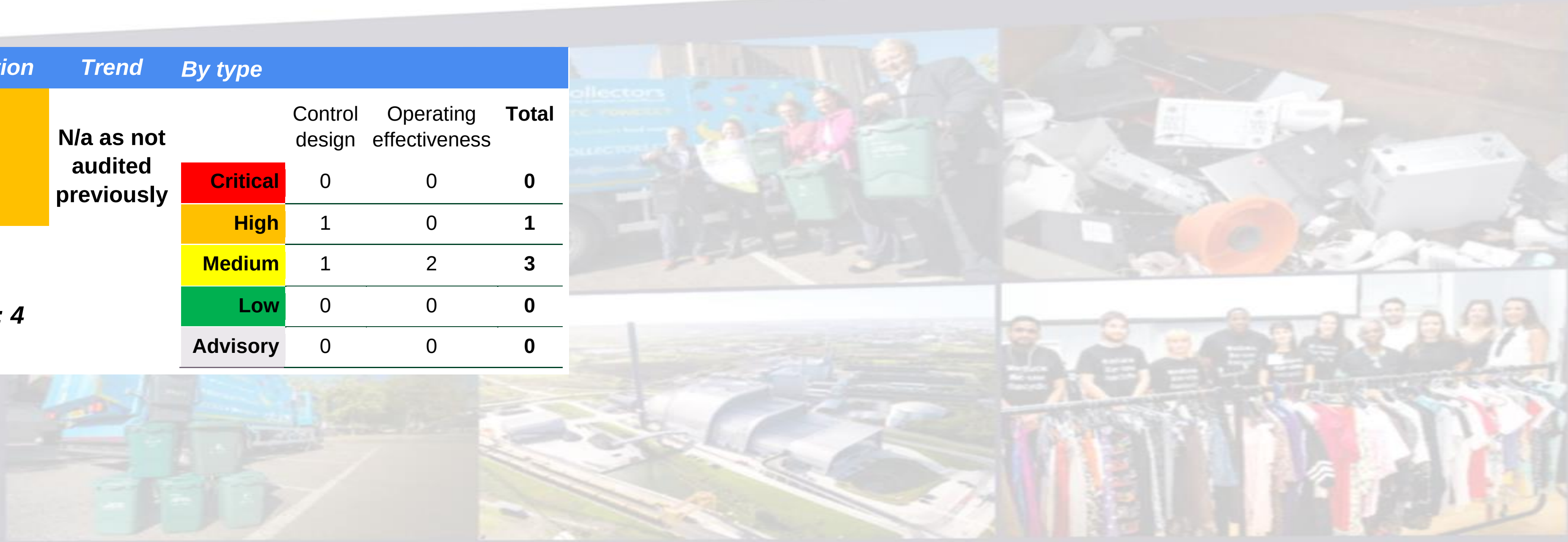
West London
Waste Authority

Final
February 2024

Internal Audit Report 2023/24

Cyber (Business/Operational Side) Audit

Classification	*Trend*	*By type*	Control design	Operating effectiveness	**Total**
Limited	**N/a as not audited previously**	**Critical**	0	0	**0**
		High	1	0	**1**
		Medium	1	2	**3**
Total findings: 4		**Low**	0	0	**0**
		Advisory	0	0	**0**



West London Waste
Treating waste as a valuable resource

Executive summary (1 of 2)

Summary of findings

This audit has been undertaken as part of the WLWA 2023/24 Internal Audit Plan. The WLWA have outsourced their IT to an IT managed service provider.

All organisations are now a collection of digital and physical assets, people and processes which are digitally connected to the rest of the world and thus increasingly at risk from manipulation or compromise from various cyber threats.

Cyber-attacks have become more organized and sophisticated resulting in direct (financial losses, system downtime) and indirect damage (reputational damage, legal implications). The need for effective information and cyber security controls is clear. Without them, it is difficult to protect sensitive data, and therefore, enable effective operations. Whilst the IT provider will assist with the technical side of cyber, the business side of operations need to have processes and controls in place to reduce the risk of attack and how to respond if an attack is successful.

The focus of the work is around cyber risks, assets, IT provider, security, and education on the business side.

We have raised actions to mitigate one high risk and three medium risk findings.

Key findings

We identified the following one high and three medium risk findings.

High Risk

- Cyber risks have not been assessed and the IT Strategy is out of date.

Medium Risks

- There is no Asset Inventory for the WLWA systems, and an incident response plan or contingency plans are not in place for cyber-attack recovery.
- There are weaknesses in the contractual relationship with the IT provider.
- Staff are not fully aware of cyber risks and the implications of security breaches.

Executive summary (2 of 2)

1	*Cyber Risks and IT Strategy*	High
2	*Asset Inventory, Incident Response and Contingency Plans*	Medium
3	*Contract Performance*	Medium
4	*Staff Education / Training*	Medium

By Scope Area

	Critical	High	Medium	Low	Advisory
Cyber Risks	0	1	0	0	0
Assets	0	0	1	0	0
IT Provider	0	0	1	0	0
Security	0	0	0	0	0
Education	0	0	1	0	0
Total	**0**	**1**	**3**	**0**	**0**

Background and scope (1 of 2)

Background

The West London Waste Authority (WLWA) are responsible for disposing of waste for six London Boroughs.

- London Borough of Brent
- London Borough of Ealing
- London Borough of Harrow
- London Borough of Hillingdon
- London Borough of Hounslow
- London Borough of Richmond upon Thames

The WLWA also receive and send data to above Councils and security of data is vitally important.

The WLWA run the Brent Household Refuse and Recycling Centre where local residents and businesses take their unwanted items or materials.

Kick IT Services have provided a managed service to the WLWA since the 1st of June and the agreement in place expires on the 31st of May 2024.

Background and scope (2 of 2)

Scope

The audit work focused on the following areas –

Cyber Risks

- Cyber risks are fully documented in a cyber policy.
- The WLWA have a fully agreed IT Strategy which includes cyber risks.
- The cyber documents are reviewed regularly to reflect the current position and arrangements.

Assets

- Assets are identified and ownership assigned.
- Incident response and contingency plans are in place for data and system assets.

IT Provider

- A contract is in place.
- Key performance indicators are in place.
- Contract management is in operation.
- Management reports are produced regularly and discussed.
- Patches are implemented within seven days.
- Back up processes are in place to mitigate the risks of data loss.

Security

- Access controls are in place.

Education

- Staff are fully aware of cyber risks and controls in place to adhere to.

Limitation of scope

Our work was limited to the sub-processes and control objectives outlined above.

The scope of our work also did not cover IT controls and processes, such as interfaces.

Management should be aware that our internal audit work was performed in accordance with Public Sector Internal Audit Standards 2017 (PSIAS) and the Local Government Application. The assurance grading provided in our internal audit reports are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board. Our internal audit testing was performed on a judgemental sample basis and focussed on key controls mitigating risks. Our testing was designed to assess the adequacy and effectiveness of key controls in operation at the time of the audit.

Please note that in relation to the scope above, whilst our internal audit assessed the efficiency and effectiveness of key controls from an operational perspective, it is not within our remit as internal auditors to assess the efficiency and effectiveness of policy decisions.

Current year findings (1 of 4)

Cyber Risks and IT Strategy

Control Design & Operational Effectiveness

1

High

Finding and root cause

The WLWA have not performed a cyber risk assessment to date. The assessment could prompt the need for mitigating controls to reduce the risk of an attack and the severity. There is an IT provider managing the technical service but there are still spam emails coming through and cyber risks to mitigate.

The risk assessment results should feed back to the risk register at department and corporate levels and used to create a cyber policy, but this has yet to be undertaken.

The WLWA IT Strategy is very out of date and refers to Ealing Servers used and WLWA Head Office location in the Hounslow Civic Centre. The age of the strategy (2016) shows that regular reviews have not been undertaken as the IT information does not reflect the current technical specification and operational practices. We are aware, however, that since the start of the audit this document is currently being worked on.

Cyber-attacks are often described as complex and sophisticated and performed by expert hackers. However, the vast majority of attacks are based on well-known techniques such as phishing emails. This type of attack can be defended against if proper controls, monitoring and awareness are in place and followed.

Implications

- High risk of cyber-attacks due to poor controls or a lack of robust controls in place.

Action plan

1) A cyber risk assessment will be undertaken, and the results used to tighten controls and fed back to the current risk register.
2) A new IT Strategy is created which matches the current and future plans of the WLWA.
3) A cyber policy is created and agreed.
4) All IT and cyber related documents are regularly reviewed to remain relevant.

Responsible person/title

Xenab Khan (Project / Finance Manager)

Target date

30th June 2024

West London Waste

Treating waste as a valuable resource

Current year findings (2 of 4)

Asset Inventory, Incident Response and Contingency Plans

Control Design

2

Medium

Finding and root cause

Cyber-attacks can be defended in two ways.

1. Cyber Security – the technical defence to stop hackers entering your systems and causing issues.
2. Cyber Resilience – where the business can defend themselves, detect potential attacks and respond to and recover from a cyber-attack.

An IT asset inventory allows the WLWA to know what the company's critical IT assets are, who is responsible for each asset, what it is used for and where it is stored.

Different assets hold a contrasting importance to keep the business-as-usual position.

The corporate risk register has identified that cyber-attacks could result in –

- Data Loss.
- Failure to make statutory reports.
- Relying on Boroughs or suppliers for invoicing data.
- Operational shocks or project delays.

The above risks should be examined against the assets to determine what the implications are likely to be when compromised and what the business can do to prevent issues. Assigning an owner to each system asset can provide a more accurate picture. Assets which hold customer details need privacy defence whilst borough financial information need tight controls around unauthorised access. The Authority need to also know age of IT assets to ensure that they remain supported, and patches can be applied.

There is a contract in place to manage the IT service which has cyber-attack defences in place, but we found no reliance plans on the business operational side.

The WLWA do not have an incident response plan and we were not provided with any contingency plans to ensure the day-to-day work by the business has minimal disruption during and after a cyber-attack.

Implications

- Slow recovery from incidents where ownership of assets is not formalised and staff being unaware of what to do.
- Critical systems are not recovered promptly where they have not been prioritised.
- Financial loss due to down time.
- Projects unable to deliver on time.
- Unsupported assets with inadequate security/updates.
- Supplier and customers unaware of issues causing increased calls and service dissatisfaction leading to reputational damage.

Action plan

1) We will create an IT asset inventory and responsibility will be assigned.
2) An incident response plan will be created and shared with staff. The plan should be regularly tested and reviewed.
3) Contingency plans after a cyber-attack should be written alongside the incident response plan. Consideration of key systems and the priority in which they are recovered is included. These needs to be shared with relevant staff.
4) This plan should also be tested and reviewed regularly

Responsible person/title
Xenab Khan (Project / Finance Manager)
Target date
30th Sept 2024

Current year findings (3 of 4)

Contract Performance

Control Design and Operational Effectiveness

3

Medium

Finding and root cause

There is a contract for managed IT services with Kick. The service agreement lists out what is covered and what is possibly not which needs clarification. As an example, within the cover, it states - Business Continuity / Disaster Recover (monitor operation of environment and restore to working environment) is dependent on whether or not the customer has current business continuity offering from Kick.

The contract contains deliverable services which are not currently monitored to determine if Kick are meeting the agreed service agreement. The contract monitoring meetings are not currently minuted.

The WLWA Contract Manager repeatedly challenged Kick as they have not provided any management information data on their deliverables which could be used to create KPI's. These conversations have recently resulted in a change of account manager and Kick started to produce call logs for the WLWA, but these still do not contain enough information to measure performance. The service agreement has levels of priority for calls and a set turnaround time for them to resolve. The report provided only gives the date and time the call was made and a description. There is no information on the priority levels and the date and time the issue was resolved. The WLWA Contract Management has produced a template that she wants Kick to populate but this is not yet being used.

There is no information provided by Kick to give assurance that patches are applied quickly, and backups have been taken and retained for 1 month as detailed in the service agreement. Recent hacks have included issues where a virus has been dormant for a period of time and the virus is included in the back-up. This risk may be discussed with the supplier to ascertain if it could occur.

Kick have reportedly implemented a process where system accounts are disabled after 90 days of inactivity, but we were not provided any evidence that this has happened, and results reported to the WLWA Contract Manager.

Implications

- Poor performance by provider goes unnoticed leading to technical issues in the event of an attack.
- Exposure to technical risks if the contract does not cover all required services.
- Slow recovery of systems if certain services are not covered in the service agreement.

Action plan

1) The Contract Manager will meet with the Kick Account Manager to ensure the cover purchased is adequate for the company's needs and expectations.
2) Key Performance Indicators will be designed around the service agreement deliverables and the provide will be told to provide the information required.
3) Contract Monitoring meetings are minuted and retained.
4) Kick will be asked to provide reports on their monthly activities.
5) Results from the 90-day scan will be reported monthly.
6) We will discuss the back-up arrangements with Kick to see if the risk of it backing up the virus is adequately managed.

Responsible person/title
Xenab Khan (Project / Finance Manager)
Target date
30th June 2024

Current year findings (4 of 4)

Staff Education / Training

Operational Effectiveness

4

Medium

Finding and root cause

An important factor in cyber defence is staff awareness of risks and how they can help reduce attack opportunities.

There is some education provided to staff but it’s not comprehensive. Examples of gaps are -

- Staff need to be wary of working on WLWA documents on their personal computers which may not carry the same level of security as WLWA systems do.
- General Data Protection Rules (GDPR) which includes rules relating to cyber.
- Consequence of opening attachments which carry viruses or spyware.
- Cyber risks in general.

We were advised that GDPR training was provided to a small number of staff but was not rolled out to all staff as planned.

A two-factor authentication process to access WLWA systems is in place and alert banners are displayed when emails are from outside of the company. However, there is no training in place or cyber risk documents to refer to.

Implications

- Breaches in GDPR rules leading to financial and reputational damage.
- Contaminated data or viruses entering the system due to human errors / ignorance leading to business disruption.
- Deadlines for statutory returns etc missed.

Action plan

1) Staff training is provided to all staff.
2) GDPR is rolled out to staff members.
3) A comprehensive guideline document is produced for staff to refer to.

Responsible person/title
Xenab Khan (Project / Finance Manager)
Target date
31st December 2024

Appendix A: Basis of our classifications

Individual finding ratings

Critical

A finding that could have a:

- ***Critical*** *impact on operational performance; or*
- ***Critical*** *monetary or financial statement impact; or*
- ***Critical*** *breach in laws and regulations that could result in material fines or consequences; or*
- ***Critical*** *impact on the reputation or brand of the organisation which could threaten its future viability*.

High

A finding that could have a:

- ***Significant*** *impact on operational performance; or*
- ***Significant*** *monetary or financial statement impact; or*
- ***Significant*** *breach in laws and regulations resulting in significant fines and consequences; or*
- ***Significant*** *impact on the reputation or brand of the organisation*.

Medium

A finding that could have a:

- ***Moderate*** *impact on operational; or*
- ***Moderate*** *monetary or financial statement impact; or*
- ***Moderate*** *breach in laws and regulations resulting in fines and consequences; or*
- ***Moderate*** *impact on the reputation or brand of the organisation*.

Low

A finding that could have a:

- ***Minor*** *impact on the organisation's operational performance; or*
- ***Minor*** *monetary or financial statement impact; or*
- ***Minor*** *breach in laws and regulations with limited consequences; or*
- ***Minor*** *impact on the reputation of the organisation.*

Appendix B: Limitations and responsibilities

Limitations inherent to the internal auditor’s work	
We have 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 judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.	***Future periods*** Our assessment of controls is for the period specified only. Historic evaluation of effectiveness is not relevant to future periods due to the risk that: • The design of controls may become inadequate because of changes in operating environment, law, regulation, or other changes; or • The degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management’s responsibility to develop and maintain sound systems of risk management, internal control, and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management’s responsibilities for the design and operation of these systems.

We endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we 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, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist.