



SOUTH YORKSHIRE MAYORAL COMBINED AUTHORITY

IT Asset Management

Revised Final Internal Audit Report: 4.24/25

9 September 2024

This report is solely for the use of the persons to whom it is addressed.

To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party.

Annex B

CONTENTS

Audit outcome overview	3
Summary of management actions	6

Appendices

Detailed findings and actions	8
Appendix A: Categorisation of findings	12
Appendix B: Scope	13





AUDIT OUTCOME OVERVIEW

In line with our scope, included at Appendix C, the overview of our findings is detailed below.

Conclusion: Our testing highlighted that the MCA has established controls and processes for the management of IT assets. An annual process to plan for the disposal of hardware that has reached the end of its useful life and to procure new IT equipment had been established. This is supported by tools such as Asset vision and Auvic network monitoring that alert the IT team should any new hardware be connected to the MCA's IT environment. IT assets have ownership established and recorded in the IT asset register Hornbill and maintenance routines are in place to keep IT assets up to date. Nessus vulnerability scans are regularly conducted to identify additional patching requirements.

However, there is no defined escalation process when leavers do not return the IT equipment issued to them. This is a potential risk where remote workers are outside of South Yorkshire. There is currently no documented process when a member of staff leaves the MCA in a non-standard way, such as through disciplinary action, if they are put on gardening leave or if they are a contractor. There has been one instance where IT equipment (laptop) has not been returned and could result in financial loss to the MCA. Upon termination, all access to SYMCA's systems is blocked therefore there is minimal risk of unauthorised access to the data should the leaver continue to try to access a laptop they have not returned or if it is lost or stolen. Other minor control improvements were identified on formalising the scheduling a rolling audit of IT asset register and the timely deletion of data from devices collected for disposal which were in the process of being implemented at the time of the audit.

Internal audit opinion:

 Minimal Assurance	 Partial Assurance	 Reasonable Assurance	 Substantial Assurance
---	---	--	---

Taking account of the issues identified, the board can take reasonable assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.

However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified risk(s).

Audit themes: Retrieval and recording of IT Assets:

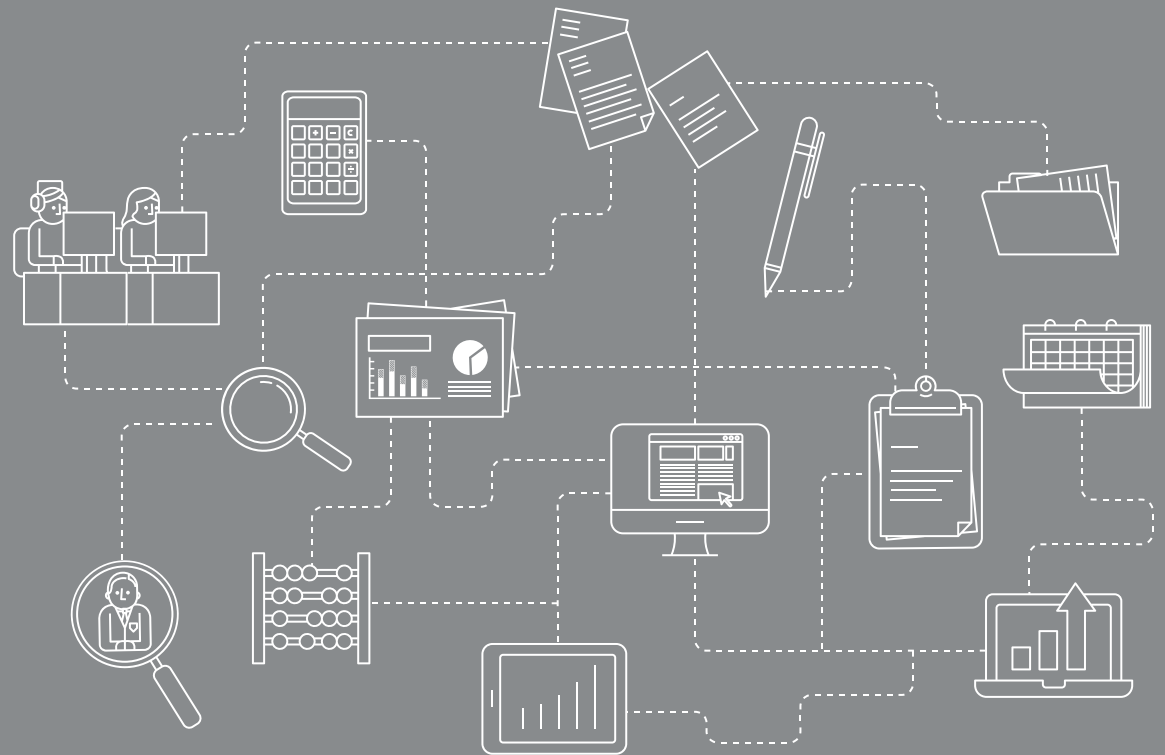
- There is a lack of formal processes and control over leavers that do not return IT assets in a timely manner following their employment at the MCA. This is particularly relevant for non-standard leavers such as contractors or those that leave following a disciplinary. This could lead to the loss of equipment. **Low**
- All IT hardware assets are recorded in the IT asset register, Hornbill. This records information on each asset, its unique identifying code and the responsible owner of each IT asset.
- Annual planning for IT assets that require replacing takes place and is budgeted for as part of the business planning process. Procurement frameworks such as Health Trust Europe and G-Cloud are used to procure IT assets from trusted providers.

Policy, procedures and documentation:

- Informal rolling audits of the IT asset register and inventory are conducted, however the requirement to conduct such audits has not been documented. This increases the risk of the audits not taking place should there be any turnover of staff. **Low**
- Standard Operating Procedures for the maintenance of IT hardware assets have been documented, however they are still in draft form and there is no clear owner with responsibility for aligning the maintenance of IT hardware with good practice. **Low**
- The process to manage the secure disposal of IT hardware assets such as laptops has not been formally documented in a standard operating procedure or the Standard for Asset Management (IT09). The process followed in practice to re-image and wipe laptops prior to disposing of them is satisfactory, however, the absence of a formal process to guide what should be done increases the risk of data and access of the MCA's IT systems not being formally removed. **Low**

Summary of Actions for Management

01



SUMMARY OF MANAGEMENT ACTIONS

The action priorities are defined as*:

High

Immediate management attention is necessary.

Medium

Timely management attention is necessary.

Low

There is scope for enhancing control or improving efficiency.

Ref	Action	Priority	Responsible Owner	Date
1	Management will document a formal schedule to conduct hardware asset audits. This will include populating the "Last Audited" field in Hornbill for hardware assets and using this date to schedule future audits of hardware.	Low	Digital Services Manager	31 March 2025
2	Management will standardise the process between departments to chase leavers for IT assets and when escalating to the Finance and Legal teams. This will be documented in a standard operating procedure on the Issue and Recovery of DTS Kit and include provisions for collecting IT assets from non-standard leavers following gardening leave or a disciplinary process.	Low	Head of HR Operations	31 December 2024
3	Management will complete, review and approve the Standard Operating Procedure Manual. This will include verifying the information within the Manual is reflective of good practice, embedded into business as usual operations and completing the document control section of the Manual.	Low	Cyber Resilience & Information Governance Manager	31 December 2024
4	Management will document the agreed process to re-image, wipe and eventually dispose of IT equipment such as laptops.	Low	Technical Services Manager	31 December 2024

* Refer to Appendix B for more detail

DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all audit testing undertaken.

Background / Why we did the audit

As part of the 2024/25 Internal Audit Plan, we conducted a review to assess how South Yorkshire Mayoral Combined Authority (the MCA) manages IT hardware assets. We reviewed the controls and processes in place over how the MCA procures new IT hardware, monitors and maintains the hardware connected to the IT environment, and eventually disposes of IT hardware that reaches the end of its useful life. The full scope of this audit can be found in Appendix B.

A complete and accurate understanding of the technology that makes up an organisation's IT environment is a crucial first step when developing a robust cyber security framework. Without an understanding of an organisation's digital footprint and the perimeter of the IT environment, it is more challenging to establish an effective security control framework. Identifying and recording the existence and location of IT assets is one of the foundational building blocks in security frameworks such as the National Cyber Security Centre's (NCSC) 10 Steps to Cyber Security and the first domain in the National Institute for Technology and Standards (NIST) Cyber Security Framework (CSF).

Area: IT Asset Audits

Control	<p><u>Partially missing control</u></p> <p>Informal rolling audits of the IT asset register are conducted, however the schedule for these audits has not been documented.</p>	<p>Assessment:</p> <p>Design ×</p> <p>Compliance N/a</p>
Findings / Implications	<p>It was noted that hardware asset audits are conducted on a rolling programme throughout the year, on approximately a yearly basis, however, the rolling audits have been not fully formalised. Steps have been taken to enable the tracking of asset audits within the asset register Hornbill, but this is still in the process of being fully populated on Hornbill. Until such audits are formally scheduled and the new Last Audited field has been populated for all IT hardware assets, there is an increased risk that assets are overlooked, and missing or damaged assets are not identified in a timely manner. This could lead to increased costs and negatively impact the MCA's ability to effectively plan for future hardware asset needs.</p>	
Management Action 1	<p>Management will document a formal schedule to conduct hardware asset audits. This will include populating the "Last Audited" field in Hornbill for hardware assets and using this date to schedule future audits of hardware.</p>	<p>Responsible Owner: Digital Services Manager</p> <p>Date: 31 March 2025</p> <p>Priority: Low</p>

Area: Retrieval of IT Assets

Control	<p><u>Partially missing control</u></p> <p>The HR team contact new starters and leavers when issuing and collecting IT equipment from staff respectively; this includes items such as laptops, keyboards, mice and headsets. When issuing equipment new starters sign for each item issued, and this is then recorded in Hornbill, the hardware asset register. When collecting equipment from leavers, the IT team provides a list of the equipment issued to that member of staff upon request to HR who in turn notify the leaver of what they must return and the date it will be returned. If equipment is not returned on the agreed date the IT team notifies HR. However the escalation process in situations where leavers do not return IT equipment has not been formally agreed between different departments.</p>	Assessment: Design × Compliance N/a			
Findings / Implications	<p>While the process to issue and retrieve IT assets has been documented, it has not been embedded into the Standard for Asset Management (IT09) and has no clear review or approval to confirm ownership of this process and that it aligns to current practice. This increases the risk that this process has not been formally agreed between the different teams involved (Digital Services, People Services, Finance and Legal) and of it not being followed in practice.</p> <p>We noted that challenges have been encountered in the escalation process if IT equipment is not returned by leavers in a timely manner. When escalating the issue of leavers not having returned IT equipment, we were advised that this should be escalated via their line manager and eventually to the Finance and Legal teams. We were informed that in one case this procedure was not followed, leading to the loss of equipment. IT equipment not being returned to the MCA increases the risk of financial costs to replace those IT assets. The potential for unauthorised access to the data is minimal as systems are blocked and accounts disabled. Furthermore, we noted there was no formally agreed process in place for the return of IT assets from non-standard leavers. There is limited guidance on the collection of IT assets of staff that leave the MCA following gardening leave, a disciplinary process. The retrieval of IT assets could potentially become a greater issue where remote workers are located outside of South Yorkshire.</p>				
Management Action 2	<p>Management will standardise the process between departments to chase leavers for IT assets and when escalating to the Finance and Legal teams. This will be documented in a standard operating procedure on the Issue and Recovery of DTS Kit and include provisions for collecting IT assets from non-standard leavers such as contractors and following gardening or a disciplinary process.</p>	<table border="0"> <tr> <td data-bbox="1400 1029 1635 1201"> Responsible Owner: Head of HR Operations </td> <td data-bbox="1635 1029 1926 1201"> Date: 31 December 2024 </td> <td data-bbox="1926 1029 2148 1201"> Priority: Low </td> </tr> </table>	Responsible Owner: Head of HR Operations	Date: 31 December 2024	Priority: Low
Responsible Owner: Head of HR Operations	Date: 31 December 2024	Priority: Low			

Area: Disposal of IT Assets

Control	A Standard Operating Procedure Manual has been drafted for the maintenance of IT hardware. This includes the patching and update processes to maintain hardware Operating Systems and firmware.	Assessment:		
		Design		✓
		Compliance		×

Findings / Implications	The Standard Operating Procedure Manual is in draft and the version control has not been fully populated, which has resulted in there being no clearly assigned owner for the processes set out in the Manual. This increases the risk that the processes set out in the Standard Operating Procedure Manual may not reflect good practice or what occurs in practice. This could lead to IT assets not being maintained, resulting in vulnerabilities to the MCA's IT environment.
--------------------------------	---

Management Action 3	Management will complete, review and approve the Standard Operating Procedure Manual. This will include verifying the information within the Manual is reflective of good practice, embedded into business as usual operations and completing the document control section of the Manual.	Responsible Owner: Cyber Resilience & Information Governance Manager	Date: 31 December 2024	Priority: Low
----------------------------	---	--	----------------------------------	--------------------------------

Area: Disposal of IT Assets

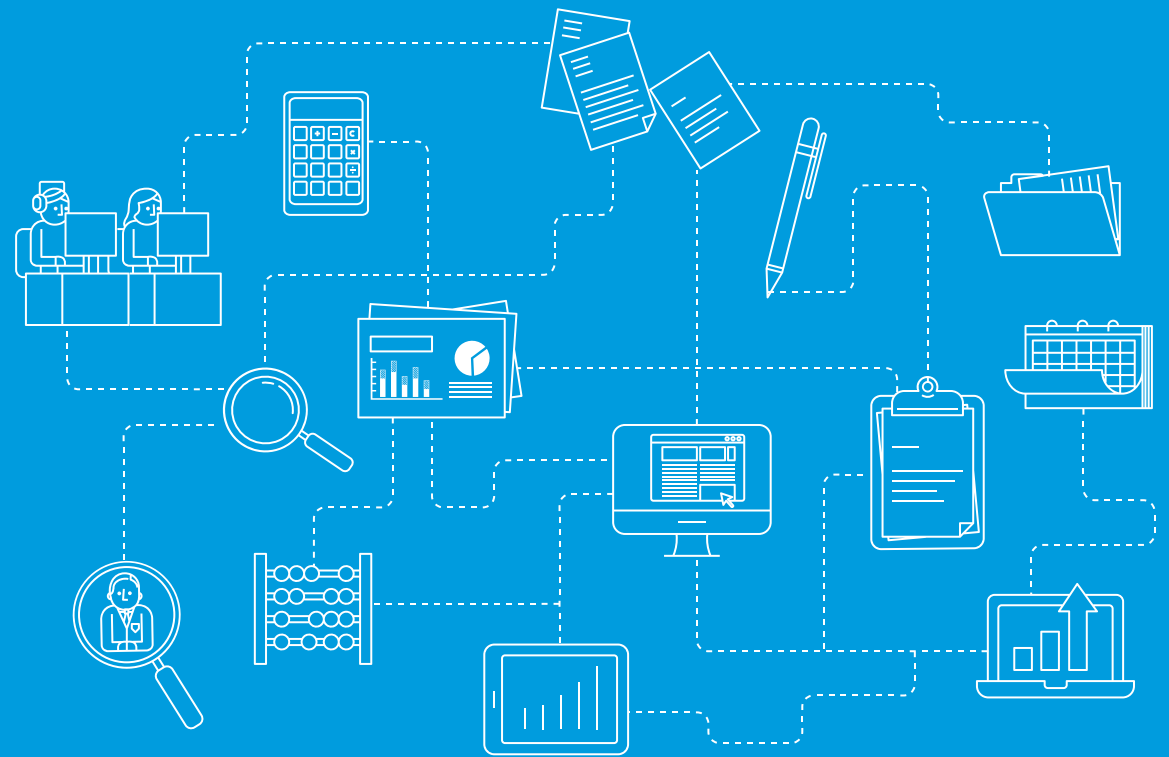
Control	Laptops that reach the end of their useful life are marked for disposal in the IT asset register and collected by the IT team. Once collected they are re-imaged to remove any applications that have been installed and any data saved locally. Prior to being disposed of with a third party, laptops are wiped to remove access to the MCA's IT environment.	Assessment:		
		Design		✓
		Compliance		×

Findings / Implications	The process for re-imaging returned laptops and wiping them prior to disposal has not been formally documented in a standard operating procedure or the Standard for Asset Management (IT09). The absence of a formal process on how laptops should be disposed increases the risk the agreed process is not followed in practice, particularly should there be any turnover in staff, which could result in data remaining on devices for an extended period of time, which may lead to its loss in the event that laptops are stolen or accessed by malicious actors prior to their collection for disposal.
--------------------------------	--

Management Action 4	Management will document the agreed process to re-image, wipe and eventually dispose of IT equipment such as laptops.	Responsible Owner: Technical Services Manager	Date: 31 December 2024	Priority: Low
----------------------------	---	---	----------------------------------	--------------------------------

Appendices

03



APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings

Low

There is scope for enhancing control or improving efficiency.

Medium

Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.

High

Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The following table highlights the number and categories of management actions made as a result of this audit.

Risk	Control design not effective*	Non-compliance with controls*	Agreed actions**		
			Low	Medium	High
Heightened Cyber Security Threat	2 (8)	2 (8)	4	0	0
		Total	4	0	0

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

APPENDIX B: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the following risk:

Objective of the risk under review	Risks relevant to the scope of the review	Risk source
To ensure the organisation's assets are accounted for, deployed, maintained, upgraded, and disposed of when the time comes. Includes hardware, software systems, or information an organisation places value upon.	Heightened Cyber Security Threat	Corporate risk register

When planning the audit, the following were agreed:

Areas for consideration:

- **Asset Identification:** Review the processes and tools in place to scan for and identify what hardware is connected to SYMCA's IT network and processes data.
- **Issuing and Retrieval of IT Equipment:** Review of the processes in place for issuing and collecting IT equipment from staff.
- **Asset Registers:** Up to date asset registers are in place for hardware and software.
- **Asset Ownership:** Assessment of the assignment of ownership and accountability for each asset to specific individuals or departments.
- **Planning:** Assessment of the processes in place for identifying the need for IT assets based on organisational requirements, and the development of strategy and budget for acquiring IT assets. This includes lifecycle planning, i.e., how assets' eventual replacement or upgrade are accounted for.
- **Asset Procurement and Management:** Assessment of the procedures for procuring IT equipment and ongoing physical inventory checks.
- **Maintenance of IT Hardware:** Review the standard operating procedures in place for the maintenance and upkeep of IT hardware including user endpoints and network infrastructure (i.e. Operating System and firmware patching).
- **Disposal:** Assessment of the processes for decommission and secure disposal of assets, including removal of sensitive data (data sanitisation) from assets where necessary.

Limitations to the scope of the audit assignment:

- All testing will be performed on a walkthrough basis, where applicable.
- This review will not assess the accuracy and completeness of the IT asset management process, but rather the processes and controls involved in the identification, monitoring, and management of IT assets.
- The scope of this review will cover IT hardware assets only and will not look at wider asset management or operational technology.

- We will not provide assurance on the completeness of the IT asset register.
- We will not confirm the existence of all assets listed on the register.
- We will not provide assurance on whether SYMCA is achieving value for money.
- We will not comment on the decisions made in respect of SYMCA's purchases or the selection of suppliers, and we will not provide assurance that purchasing decisions meet the needs of the organisation.
- We will not provide assurance that assets used by the SYMCA will protect against all vulnerabilities.
- This review will not assess licencing or licence management.
- The results of our work are reliant on the quality and completeness of the information provided to us.
- Our work will not provide an absolute assurance that material errors, loss or fraud do not exist.
- Please note that the full scope of the assignment can only be completed within the agreed budget if all the requested information is made available at the start of our fieldwork, and the necessary key staff are available to assist the internal audit team. If the requested information and staff are not available we may have to reduce the scope of our work and/or increase the assignment budget. If this is necessary we will agree this with the client sponsor during the assignment.
- To minimise the risk of data loss and to ensure data security of the information provided, we remind you that we only require the specific information requested. In instances where excess information is provided, this will be deleted, and the client sponsor will be informed.

Debrief held 16 August 2024
Draft report issued 22 August 2024
Responses received 6 September 2024
 9 September 2024

Final report issued 9 September 2024
Revised final report issued 9 September 2024

Internal audit Contacts Robert Barnett, Head of Internal Audit
 Anastasia Mullen, Associate Director IA
 Aaron Macdonald, Manager IA
 Wil Milligan, Manager Technology Risk Assurance (TRA)
 Charley Mather, Senior Consultant TRA

Client sponsor Gareth Sutton, Executive Director Resources and Investment
 Nick Brailsford, Assistant Director Digital & Technology Services

Distribution Gareth Sutton, Executive Director Resources and Investment
 Nick Brailsford, Assistant Director Digital & Technology Services

We are committed to delivering an excellent client experience every time we work with you. If you have any comments or suggestions on the quality of our service and would be happy to complete a short feedback questionnaire, please contact your RSM client manager or email admin.south.rm@rsmuk.com.

FOR FURTHER INFORMATION CONTACT

Rob Barnett, Head of Internal Audit

Email: Robert.Barnett@rsmuk.com

Anna Mullen, Associate Director

Email: Anasatasia.Mullen@rsmuk.com

Aaron Macdonald, Manager

Email: Aaron.Macdonald@rsmuk.com

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of South Yorkshire Mayoral Combined Authority, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM UK Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM UK Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.