TRANSPORT FOR THE NORTH

IT and Remote Working Asset Management

Internal audit report 1.23/24

Final

3 July 2023

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

1. EXECUTIVE SUMMARY

With the use of secure portals for the transfer of information, and through electronic communication means, 100 per cent of our audit has been conducted remotely. Remote working has meant that we have been able to complete our audit and provide you with the assurances you require. Based on the information provided by you, we have been able to sample test to complete the work in line with the agreed scope.

Why we completed this audit

Transport for the North are currently in the process of preparing for an office relocation. In preparation for this, it was agreed that RSM would conduct on audit on the management of IT and Remote Working Assets.

TfN's Information Technology Manager and Head of Facilities came into post from September 2022 and have recently reviewed the organisation's Asset Management Policy and Procedure (April 2023). The document includes the processes, practices, and procedures in relation to the purchase, control and disposal of all IT equipment and furniture assets to ensure that accountability and Value for Money (VfM) with regards to the effective management of all such assets is established and maintained at all times.

A new IT helpdesk system, Mojo software (which has an integrated asset management module) has also been implemented, which is utilised for the management and recording of assets. This is overseen and managed by the Information Technology Manager. TfN currently has 115 members of staff and 554 assets in total (consisting of laptops, monitors, phones and audio-visual equipment)

The purpose of the review was to consider how TfN physically manages IT and Remote Working Assets, recognising the improvements that the Information Technology Manager and Head of Facilities have implemented since coming into post.

Conclusion

Our review has confirmed that a full reconciliation/ verification of the assets recorded on the Mojo system has been undertaken by the Information Technology Manager, with assistance of the Facilities Manager in March 2023 to ensure the accuracy of the data and to identify any issues.
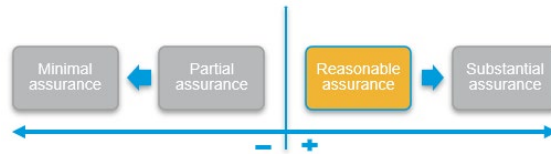
Additionally, we have confirmed that TfN has an Asset Management Policy and Procedure, which has recently reviewed and updated (April 2023), however through our review and testing undertaken, we have identified that further review of the Asset Management Policy and Procedures is required.

We also noted that, as part of a full reconciliation process completed in March 2023, it was identified that 12 laptops had not been returned to TfN, following on from a member of staff leaving. Through the use of the Azure software, emails and telephone calls, where possible, three had been retrieved. However, at the time of review, there remained nine laptops still to be retrieved. Through discussions with the Information Technology Manager, we confirmed that they were actively pursuing these machines. Through our audit work, we are also aware that controls have now been implemented to limit the risk of this occurring in the future. As such, we have not raised a management action specifically in regards to the nine laptops which have not been retrieved.

Our review has resulted in one 'medium' priority and two 'low' priority management actions being raised. Full details of our findings are included in section 2 of this report.

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).

Key findings

We identified the following findings:

TfN has a recently revised Asset Management Policy and Procedure relating to the IT and Remote Working asset management requirements. The Policy and Procedure has been approved for publication by the Head of Facilities. As part of the review, we have identified that the appendices including both starter and leaver forms do not reflect the current forms utilised as part of the process and that the Policy and Procedure does not state the frequency of when the asset reconciliation/ verification process should be undertaken. As such, we have raised a management action.

TfN has an IT starter form that is completed for all newly appointed members of staff, which includes new employer details, devices required and system access levels. We performed testing of 10 newly appointed members of staff and by review of the IT starter form identified that in one case the form had not been signed by a member of the HR Department.

TfN has an IT leaver form that is completed for all members of staff leaving TfN. The form should be signed by a member of the HR Department and submitted to the IT Department *'no less than five working days in advance'.* We performed testing of 10 leavers and identified the two forms that had not been signed by a member of HR Department and in four cases the form had not been submitted to the IT Department at least five working days of the member of staff leaving.

In both the case of the IT starter and leaver forms, we noted that the forms used differs to that attached to the Policy and Procedure. Additionally, the current forms require approval from two members of staff, however it was confirmed that only a member of the HR Department needs to approve both types of form.

It is the responsibility of the Information Technical Manager to ensure that the monitoring/ reconciliation of assets takes place. At the time of review, it was noted that a full reconciliation of assets recorded on the Mojo system had taken place in March 2023. For a sample of 10 assets, we confirmed that as part of the process that in all cases the asset had been verified to the Mojo system, either physically or by email verification by the user.

It was noted that, as part of the reconciliation process, that a number of laptops had not been returned to TfN, following on from a member of staff leaving. Through the use of the Azure software, emails and telephone calls where possible three had been retrieved, however at the time of review there remained nine laptops still to be retrieved. Through discussions with the Information Technology Manager, we confirmed that this was an active ongoing process. As such, we have not raised a management action.

TfN utilises the Helpdesk system, Mojo software module for the recording of assets, with a value of £50 or more. We performed testing of 10 newly appointed members of staff and confirmed that the following information had been recorded on the Mojo system:

- Description of the item/ classification;

- ID number/ serial number;

- Tag number of the asset;

- Name of member of staff asset allocated to; and

- Location i.e. remote.

In response to home-working and following on from a display screen equipment (DSE) assessment, three members of staff have been provided with an additional monitor. We confirmed that the three monitors had been recorded on the Mojo system against the individual members of staff.

It was confirmed by the Information Technology Manager and by review of a report produced from the Mojo system, that no assets have been recorded and disposed of in the last four years. Furthermore, through discussions with the Information Technology Manager, we were informed that only monitors or chairs would be formally disposed.

As laptops are on a lease deal these are not included and are kept regardless and then set in stock for re-use or prepped for sending back at the end of the lease deal. We were also informed that when assets are disposed of, it is the responsibility of the IT Team to wipe any company data. They also use Microsoft Azure to manage their devices and once removed from the portal, the device is unable to access the corporate network and the machine is reset. TfN has previously used a secure disposal recycling company to safely dispose of assets.

2. 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 internal audit testing undertaken.

Area: Policies and Procedures		
Control	Transport for North (TfN) has a Asset Management Policy and Procedure relating to IT and Remote Working asset management requirements, including office furniture and equipment. The Policy and Procedure is subject to periodic review by a member of the senior management team to ensure that they remain up to date and reflect current operating practice. The Policy and Procedure is available to all staff via the Intranet.	**Assessment:** **Design** ✓ **Compliance** ×
Findings / Implications	We obtained a copy of the latest Asset Management Policy and Procedure and by review confirmed that it was last updated in April 2023. The Information Technology Manager confirmed that the Policy and Procedures had been reviewed by the Head of Facilities and Risk Manager as part of the review process. We confirmed by review of an email that the Head of HR, acting as the Head of Facilities has approved the current Policy and Procedure. Additionally, we confirmed by review of a screenshot provided that the Policy and Procedure is available to all members of staff via the Intranet. As part of our review, we identified the following exceptions have been identified: • The standard forms currently utilised for the request of IT assets for new employees and for employees leaving the business were not referred to in the appendices in the Policy/ Procedures. • The frequency for the monitoring/ reconciliation of assets is not stated in the Policy and Procedure. • The process that is currently operating in respect of the approval of equipment for starters and leavers is not in line with the requirements as stated in the Policy and Procedure. There is a risk that if the Asset Management Policy and Procedures is not reflective of actual working practices, members of staff are not provided with the accurate information and guidance that should be applied.	

Management Action 1	Management will update the current Asset Management Policy and Procedure to ensure the inclusion of the timeliness for the verification/ reconciliations of assets to be undertaken and the process for the approval of starters and leavers, to reflect actual working practices. Additionally, the forms (appendices) should be updated to reflect actual working practices.	**Responsible Owner:** IT and Information Manager, Facilities Manager.	**Date:** 31 July 2023	**Priority:** Low

Area: New Starters		
Control	TfN has a standard form which is completed when requesting new IT equipment. The form is completed by the requester which, includes the new employee details, details of the device(s) requested and the systems for which access is required. The form is then authorised by a member of the HR Department and sent through to IT. Any amendments to existing devices/ access rights would be requested directly through to IT.	**Assessment:** **Design** ✓ **Compliance** ✕
Findings / Implications	For a sample of 10 new employees selected from a system list (Dynamics 365 system) provided by HR (June 2022 to May 2023), We performed testing to confirm that the standard form had been completed and authorised appropriately. Testing identified that for one of the 10 new employees selected, the form had not been approved by HR. In all cases the form had been dated prior to the start date. There is currently a risk that access rights are being allocated/ assigned that have not been appropriate approved in line with the employees roles and responsibilities. It was also noted that the standard form in use differs from that of the form, as stated in the Asset Management Policy and Procedure. Discussions with the Information Technology Manager has confirmed that the process for the completion of the form has been changed in that, the Head of HR has agreed that the form only requires approval through the HR Department and not the Line Manager, therefore we have taken this into consideration when undertaking testing. We have raised a management action (control 1) in respect of this finding.	

Management Action 2	The HR Department will ensure that all IT starter forms are approved by a member of the HR Department prior to sending through to the IT Department for processing. **Management Comment:** *The Head of HR has already discussed with their team and outlined this is critical to be completed on all future forms. The IT team will reject future forms without signature.*	**Responsible Owner:** Head of HR.	**Date:** 3 July 2023	**Priority:** Low

Area: Leavers		
Control	TfN has a standard form which is completed when a member of staff is leaving TfN. The form is then authorised by a member of the HR Department and sent through to the IT Department, *'no less than five working days in advance'*. It is the responsibility of the Information Technology Manager to organise the collection of assets from leavers and/ of movers, either through courier or the leaver returning the assets. This process also acts as notification for cancellation of leavers access on the system. In cases where a member of staff leaves TfN, arrangements for the retrieval of assets would only be actioned in cases where the nominal re-sale value is greater than £50 or a collective re-sale value greater than £150 applies, as stated in the Asset Management Policy and Procedure.	**Assessment:** **Design** ✓ **Compliance** ×
Findings / Implications	For a sample of 10 leavers selected from a system list (Dynamics 365 system) provided by HR (January 2022- May 2023), we performed testing and confirmed that in two out of 10 cases the leaver notification form had not been signed by a member of the HR Department prior to submission to the IT Department. Additionally, we identified four leaver notification forms were dated less than five working days of the date of leaving. One form had been dated on the same day as the date of leaving, one form had been dated three days prior to the date of leaving, two had been dated after the date of leaving. There is currently a risk that members of staff leaving TfN can still access emails/ systems if the IT has not been disabled, additionally, the assets will not be retrieved in a timely manner. It was also noted that the standard form in use differs from that of the form, as stated in the Asset Management Policy and Procedure. Discussions with the Information Technology Manager has confirmed that the process for the completion of the form has been changed in that the Head of HR has agreed that the form only requires approval through the HR department and not the Line Manager, therefore we have taken this into consideration when undertaking testing. We have raised a management action (control 1) in respect of this finding.	

| **Management Action 3** | The HR department will ensure that leaver forms are approved by a member of the HR Department prior to sending through to the IT Department for processing. Additionally, the forms will be sent through to the IT Department at least five days prior to the date of leaving.

Management Comment:
Conversation with both the HR and IT teams has taken place and the leaver form has now been updated to state that the forms will be received at least 5 working days prior to leave date to ensure timely collection of TfN equipment and user account deletion. | **Responsible Owner:**
Head of HR, IT and Information Manager | **Date:**
3 July 2023 | **Priority:**
Medium |

APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
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**
Cyber disruption/attacks to the available information and technical infrastructure. Inappropriate user access to confidential information. Access may be limited for an unknown period of time.	0	3	2	1	0
Total			**2**	**1**	**0**

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
Our review will consider how TfN manages ICT assets.	Cyber disruption/attacks to the available information and technical infrastructure. Inappropriate user access to confidential information. Access may be limited for an unknown period of time.	Corporate Risk Register November 2022

When planning the audit, the following areas for consideration and limitations were agreed:

The audit will consider the following;

Policies and Procedures

- Policies and procedures relating to IT and Remote Working asset management are in place. These are subject to periodic review to ensure that they remain up to date and reflect current operating practice.

- Guidance on IT and Remote Working asset management is clear and available to staff.

Governance of Assets:

- The process and controls in place for requesting and approving IT and Remote Working assets.

- The controls in place for the procurement, tagging and deployment of IT and Remote Working assets.

- The classification of assets (e.g. hardware/software).

Asset Monitoring:

- The framework in place to monitor and manage assets, e.g. use of a centralised software.

- The procedures in place for lost or stolen assets.

- The process in place for the monitoring of the location, status and use of IT and Remote Working assets.

- The process in place for the reconiliation of IT and Remote Working assets.

Secure Disposal of Assets:

- The awareness of asset life cycle and management of assets approaching their end-of-life and strategy and plans for replacement.

- The controls in place for ensuring a secure disposal of assets.

Asset Retrieval:

- We will assess and review the process and controls in place for the retrieval of assets from leavers and/or movers.

Limitations to the scope of the audit assignment:

- We will not comment on the appropriateness of asset disposals just that the agreed process is adequate and has been followed.

- We will not substantively re-perform reconciliations or validate the existence of all assets..

- We will not assess the effectiveness of the utilisation of assets.

- We will not consider the purchase order process during this review

- We are not performing a full review of procurement or licencing of devices.

- We will not assess the quality and/or value of assets or assess whether assets were a good investment.

- Our review will not confirm the accuracy of the figures included in the financial accounts.

- Back-up controls will not form part of this review.

- We will undertake an assessment of the adequacy of selected aspects of the control framework and undertake limited testing to confirm its operation in practice.

- Our review is limited to reviewing selected key controls in relation to IT and Remote Working Asset Management. No other areas of TfNs financial systems will be reviewed.

- We will not comment on the appropriateness of assets purchased or disposed of by TfN.

- We will not verify the existence of assets, or comment on the condition of any assets.

- We will not look at data security arrangements for assets.

Our work does not provide assurance that material error, 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 June 2023	**Internal audit Contacts**	Lisa Randall, Head of Internal Audit
Draft report issued	27 June 2023		lisa.randall@rsmuk.com / 07730 300 309
Responses received	3 July 2023		
			Alex Hire, Senior Manager
			alex.hire@rsmuk.com / 07970 641 757
			Ciaran Barker, Assistant Manager
			Ciaran.barker@rsmuk.com / 01782 216187
Final report issued	3 July 2023	**Client sponsor**	Paul Kelly, Finance Director
		Distribution	Paul Kelly, Finance Director
			Danny Chapman, Information Technology Manager