TRANSPORT FOR THE NORTH

Follow Up

Internal audit report: 1.24/25

FINAL

3 July 2024

1. EXECUTIVE SUMMARY

Background

We have undertaken a review to follow up on progress made to implement the previously agreed management actions from the following audits:

- IT and Remote Working Asset Management (1.23/24);
- Follow Up (2.23/24);
- IT Access Management Security (3.23/24);
- Staff Mental Health and Wellbeing (4.23/24); and
- Procurement - Value for Money (6.23/24).

The focus of this review is to provide assurance that actions previously raised have been adequately implemented.

Please note that no management actions were raised in our Performance Management and Appraisals (5.23/24) review.

Conclusion

Taking account of the issues identified in the remainder of the report, in our opinion Transport for the North has demonstrated **good progress** in implementing the agreed management actions included in the assignment reports considered as part of this review.

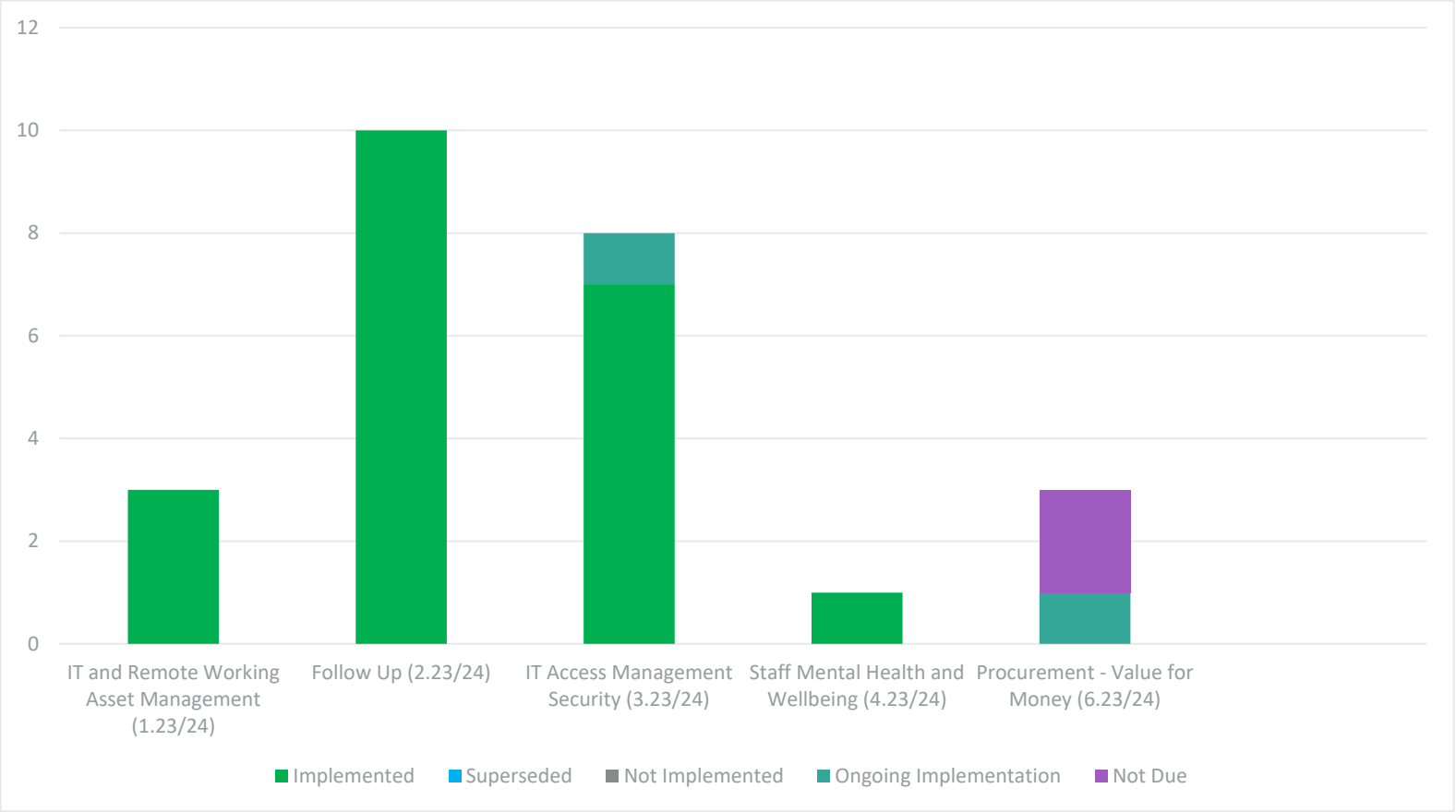
Two actions relating to the Procurement - Value for Money (6.23/24) assignment report were not due to be implemented at the time of this follow up review in May 2024 and have therefore been excluded when forming the opinion. Details of the actions not yet due are included at Appendix B of this report.

Testing identified that 21/23 (91%) of the actions considered as part of this review have been implemented, and details of the implemented actions are included at Appendix A of this report. For 2/23 (9%) management actions, we confirmed that these are ongoing, and the actions should continue to be monitored until the actions are fully implemented. Please refer to section 2 for further details.

Progress on actions

The following table includes details of the status of each management action:

Implementation status by review	Number of actions agreed	Status of management actions					
		Implemented (1)	Implementation ongoing (2)	Not implemented (3)	Superseded (4)	Not Due (5)	Confirmation as completed or no longer necessary (1)+(4)
IT and Remote Working Asset Management (1.23/24)	3	3	0	0	0	0	3
Follow Up (2.23/24)	10	10	0	0	0	0	10
IT Access Management Security (3.23/24)	8	7	1	0	0	0	7
Staff Mental Health and Wellbeing (4.23/24)	1	1	0	0	0	0	1
Procurement - Value for Money (6.23/24)	3	0	1	0	0	2	0
Total	**25**	**21**	**2**	**0**	**0**	**2**	**21**


12
10
8
6
4
2
0
IT and Remote Working Asset Management (1.23/24)
Follow Up (2.23/24)
IT Access Management Security (3.23/24)
Staff Mental Health and Wellbeing (4.23/24)
Procurement - Value for Money (6.23/24)
Implemented
Superseded
Not Implemented
Ongoing Implementation
Not Due

2. FINDINGS AND MANAGEMENT ACTIONS

Status	Detail
1	The entire action has been fully implemented.
2	The action has been partly though not yet fully implemented.
3	The action has not been implemented.
4	The action has been superseded and is no longer applicable.
5	The action is not yet due.

Assignment: IT Access Management Security (3.23/24)	

Original management action/ priority/ original date	Management will:
	• Consolidate the procedure for third party assessments into a single policy, to ensure the process for onboarding and providing access to third parties is clearly outlined, alongside TfN roles and responsibilities in this process;
	• Amend this policy to ensure that risk assessments are conducted for all third parties, rather than just those lacking ISO27001 certification;
	• Ensure organisational policies and procedures on third party assessments are adhered to before granting access to organisational systems and data;
	• Create and regularly update a third party register to detail:
	  • Notes on contract terms and the role of the third party;
	  • The internal manager of this third party relationship (contract owner);
	  • The level of access third parties have to organisational systems and data, including whether they process personal data;
	  • Whether a DPA is in place;
	  • A summary of the business case for third party access;
	  • Whether the third party complies with ISO27001; and
	  • Results of data assessments and risk assessments.
	Investigate what conditional access policies can be applied to third party access to SharePoint, such as Multi-factor Authentication, and apply conditional access policies where possible and where not, consider what additional access controls can be established.

Assignment: IT Access Management Security (3.23/24)				
Audit finding/ status	1. We confirmed that an IT Approved Domain Policy is in place. It sets out the standard criteria for evaluating whether an internet domain can be added to the approved internet domains list. 2. We obtained a copy of the Data Processing Agreement (Controller-to-Processor) between TfN and Plus Four Market Research Limited dated 16 January 2024 and by review confirmed that TfN procedures on third party assessments were followed before granting Plus Four Market Research Limited access to TfN's systems and data. We confirmed the inclusion of the following in the signed agreement (but not limited to): • Supplier's obligations; • Supplier's employees; • Security; • Personal data breach; • Cross border transfers of personal data; • Terms and termination; and • Records, audit, warranties, indemnification and notice. Further, by review of the Joint Schedule (Processing Data) document, we confirmed the inclusion of the terms for processing data at TfN between the Processor and Controller. 3. We were unable to obtain a copy of the third party register. We were informed by the Data Protection & Contracts Lawyer that this management action will be incorporated into TfN's Information Governance Framework review. As such, we have reiterated this part of the action. 4. We were provided with a walkthrough by the Information Technology Manager that Multi-factor Authentication has been implemented and this is now required for all TfN Staff upon account creation. We also confirmed that upon access to the TfN SharePoint, we (RSM) were required to authenticate our access. *2 - The action has been partly though not yet fully implemented*			
Management Action 1	**Revised Management action** Management will create and regularly update a third party register to detail: • Notes on contract terms and the role of the third party; • The internal manager of this third party relationship (contract owner); • The level of access third parties have to organisational systems and data, including whether they process personal data;	**Responsible Owner:** Governance, Data Protection & Contracts Lawyer and Information Technology Manager	**Date:** 31 December 2024	**Priority:** Medium

Assignment: IT Access Management Security (3.23/24)				
	• Whether a DPA is in place; • A summary of the business case for third party access; • Whether the third party complies with ISO27001; and • Results of data assessments and risk assessments. **Management Update:** *This management action will be incorporated into TfN's Information Governance Framework review.*			

Assignment: Assignment: Procurement - Value for Money (6.23/24)				
Original management action/ priority/ original date	The waiver approval process, and waiver reporting frequency to OBT, will be defined and will be consistent between the Procurement Policy and the Constitution. Waiver approvals and reporting to OBT will be complied with in practice.			
Audit finding/ status	At the timing of our review, the Finance Director informed us that the action was in the process of being implemented. We were provided with a copy of the Procurement Update which was presented to the June 2024 Operations Board meeting, and thereafter on a monthly basis moving forward. The report includes a wavier update, which details the waivers that have been requested and granted. Based on the progress made to date, we have revised our management action to ensure that the process is defined within and consistent between with the Procurement Policy and Constitution. *2 - The action has been partly though not yet fully implemented.*			
Management Action 2	**Management action** The waiver approval process, and waiver reporting frequency to Operations Board, will be defined and will be consistent between the Procurement Policy and the Constitution.	**Responsible Owner:** Finance Director and Head of Legal	**Date:** 31 December 2024	**Priority:** Medium

APPENDIX A: ACTIONS COMPLETED

From the testing conducted during this review we have found the following actions to have been implemented.

Assignment title	Management actions
IT and Remote Working Asset Management (1.23/24)	**Implemented** 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. (Low)
	Implemented 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. (Low)
	Implemented 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. (Medium)
Follow Up (2.23/24)	**Implemented** Risk Maturity (3.22/23) Following presentation of the Assurance slides to the Operational Board, the Risk Manager will work alongside Risk Owners for the key corporate risks to ensure the Board Assurance Framework is embedded and applied for all assurance areas. (Low)
	Implemented Equality, Diversity and Inclusion Framework (5.22/23) A framework/and or procedure will be introduced to ensure that existing policies and new TfN policies, procedures and strategies are reviewed for consideration in line with PSED and that Equality Impact Assessments (EIA) are incorporated into Policies moving forward.

Assignment title	Management actions
	The framework should consider, but not limited to: • Why an EIA is important; • When an EIA should be completed and who should complete this; • Questions to consider within the EIA template (e.g. what policy or change is being introduced, who is affected by the policy/change, what engagement with stakeholders will take place and what data will be used); • Documentation of any actions from the EIA; and • The approval process for EIAs. (Medium)
	Implemented Equality, Diversity and Inclusion Framework (5.22/23) Management will, going forward update TfN's website to include clear information on the organisation's position in respect of diversity and inclusion, ensuring transparency at all times. (Low)
	Implemented Framework for Project Management - Project Approval, Delivery and Monitoring (6.22.23) Management will review and update the Policy Development Framework (PDF) to include a definition of what is considered to be a project (based on size, spend and scope). Once updated, the PDF will be formally rolled-out and implemented to ensure that the two-step process in relation to development of projects is followed consistently and the supporting documentation completed. (Low) **Management Comment (applies to all actions raised in the Framework for Project Management - Project Approval, Delivery and Monitoring (6.22.23) assignment report)** Management has agreed to form a task and finish group from within the Senior Management Team to take forward the work on the project management framework, recognising the new operating model.
	Implemented Framework for Project Management - Project Approval, Delivery and Monitoring (6.22.23) Project Initiation Documents (PIDs) will be presented and approved as part of the project approval processes in line with the approval limits within the Scheme of Delegation and by an individual with assigned responsibility. Completed PIDs will be retained centrally within a shared drive to ensure they can be shared in case of a change in the project team. (Medium)

Assignment title	Management actions
	Implemented Framework for Project Management - Project Approval, Delivery and Monitoring (6.22.23) Management will ensure that the full Responsible, Accountable, Supportive, Consulted, and Informed (RASCI) matrix exercise is completed for all projects, giving consideration to both internal and external stakeholders. (Low)
	Implemented Framework for Project Management - Project Approval, Delivery and Monitoring (6.22.23) Management will review project management best practices and identify monitoring mechanisms which will be used consistently across projects. Once finalised templates will be developed and distributed to ensure consistency. (Low)
	Implemented Framework for Project Management - Project Approval, Delivery and Monitoring (6.22.23) Management will update the lessons learnt template to include a section in relation to benefits realisation. The completion of the lessons learnt template will then be made mandatory for Project Managers (or equivalent individual assigned responsibility) for all projects. This will include the identification of actions for improvement with action owners and intended implementation dates. Completed templates will be saved within an action log or a shared drive to enable Project Managers from across the organisation to benefit from the learnings. (Medium)
	Implemented Framework for Project Management - Project Approval, Delivery and Monitoring (6.22.23) Once completed, lessons learnt reports will be presented to a delegated relevant committee / forum for oversight and to monitor actions through to completion. (Low)
	Implemented Framework for Project Management - Project Approval, Delivery and Monitoring (6.22.23) Through discussions with Project Managers, Management will consider the value of the Interdependencies Tracker and identify based on the outcomes of discussions and the funding received from the DfT whether it will be maintained and kept up to date. (Low)

Assignment title	Management actions
IT Access Management Security (3.23/24)	**Implemented** Management will conduct user access reviews on a regular basis, by consulting with organisational units and SharePoint site owners to validate that user access aligns with job roles and responsibilities. Documentation of the review and any actions taken to adjust access will be maintained to enhance accountability and for audit purposes. (Medium)
	Implemented Management will create a policy detailing the roles and responsibilities, and processes for: • Onboarding users (including training prerequisites), amending user access, and terminating user access; and • Granting, amending, and revoking third party access to SharePoint sites.# This policy will be reviewed and approved by the highest level of delegated authority before being disseminated to the relevant stakeholders. Management should also ensure this defined procedure is followed in practice. (Medium)
	Implemented Management will: • Set contractors' access to expire in line with their contract end (leaving) date; • Ensure the contract owner and contractor are suitably notified when the account is approaching expiry; • Where access is required to be extended, this will be requested through a Service Desk ticket with suitable approval obtained; and • Ensure that the new Access Control Policy (as per Management Action 4) appropriately reflects this process. (Medium)
	Implemented Management will develop a strategy for periodic testing of the incident management procedure to validate its effectiveness, ensuring that there is a lessons learnt exercise following these tests to continually improve the plan. (Low)

Assignment title	Management actions
	Implemented Management will re-assess the risk rating associated with Data Access Reviews to ensure that it accurately reflects the current risk level, and ensure there are appropriate plans in place to mitigate this risk or formally accept a higher level of risk. (Low)
	Implemented Management will: • Delete user accounts when no longer in use; • Where there is a business case for accounts to remain disabled (i.e., not deleted), ensure requests are raised through the Service Desk as part of the leaver request; and • Establish clear policies and procedures for managing disabled accounts in order to reduce security risks and ensure they are managed appropriately based on organisational requirements. (Low)
	Implemented Ensure all account permissions align with the principle of least privilege, having only the necessary access to perform their specific functions. (Low)
Staff Mental Health and Wellbeing (4.23/24)	**Implemented** Management will ensure that all line managers, with the responsibility for supporting/ referring team members to HR in respect of mental health and wellbeing will undertake regular (every three years) up-to-date absence and wellbeing refresher training via on-line e-learning. (Low)

APPENDIX B: ACTIONS NOT YET DUE

The table below lists the management actions that were not yet due for implementation at the time of our review:

Assignment title	Management action, categorisation and agreed implementation date
Procurement - Value for Money (6.23/24)	The Procurement Policy and Consitutition will be reviewed to ensure they are reflective of current legislation. As part of this review, management will ensure that reference to OJEU thresholds is removed and replaced with UK law and thresholds. Reference to named individuals who no longer work for TfN will be removed from the Procurement Policy. In advance of the Procurement Act becoming effective (expected October 2024), the Procurement Policy and Constitution will be updated to ensure it is compliant with the new Procurement legislation. The Constitution, Procurement Policy and workflow in D365 will be aligned and will be consistent regarding the procurement thresholds and the approvals required. (Medium) **30 September 2024**
	Contract managers roles and responsibilities will be reinforced. A contract administration system will be implemented to allow consistent management of contracts across TfN and provide a mechanism for centralised review. (Low) **31 March 2025**

APPENDIX C: SCOPE

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

Scope of the review

The internal audit assignment has been scoped to provide assurance on how Transport for the North (TfN) manages the following area:

Objective of the risk under review
Management has introduced effective systems for the monitoring of implementation of agreed management actions and ensuring that these are implemented in line with the agreed timescales.

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

Areas for consideration:

To assess the degree of implementation achieved of the management actions raised in the following assignment reports:

- IT and Remote Working Asset Management (1.23/24);
- Follow Up (2.23/24);
- IT Access Management Security (3.23/24);
- Staff Mental Health and Wellbeing (4.23/24); and
- Procurement - Value for Money (6.23/24).*

The focus of this review is to provide assurance that actions previously raised have been adequately implemented.

* This will be dependent on the finalisation of the report at the time of our audit fieldwork, noting that this report is currently in draft, and some actions are not due for implementation until after our fieldwork.

Please note that no management actions were raised in our Performance Management and Appraisals (5.23/24) review.

Limitations to the scope of the audit assignment:

- The review only covers audit management actions previously made and does not review the whole control framework of the areas listed above, therefore we are not providing assurance on the entire risk and control framework;
- We will ascertain the status of management actions through discussion with management and review of the most recent management action tracking report presented to the Audit and Governance Committee;
- Where the indication is that management actions have been implemented, we will undertake limited testing to confirm this;
- Where testing is undertaken, our samples will be selected over the period since actions were implemented or controls enhanced;
- Where relevant to the management action being followed up, we will ascertain whether policies / procedures / documentation have been established but we will not assess whether these are fit for purpose;
- The results of our work are reliant on the quality and completeness of the information provided to us; and
- Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

Debrief held	27 June 2024	**Internal audit Contacts**	Lisa Randall, Head of Internal Audit lisa.randall@rsmuk.com / 07730 300 309 Alex Hire, Senior Manager alex.hire@rsmuk.com / 07970 641 757 Ciaran Barker, Assistant Manger ciaran.barker@rsmuk.com / 01782 216 187
Draft report issued	27 June 2024		
Responses received	3 July 2024		
Final report issued	3 July 2024	**Client sponsor**	Paul Kelly, Finance Director
		Distribution	Paul Kelly, Finance Director Daniella Della-Cerra-Smith, Risk Manager

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

rsmuk.com