TRANSPORT FOR THE NORTH

Follow Up

Internal audit report 7.19/20

FINAL

9 April 2020

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:

- Risk Management Framework (1.18/19)
- Payment Authorisation Processes, Expenses and Use of Procurement (2.18/19)
- Procurement Framework (3.18/19)
- IT Audit – Cyber Security Controls (4.18/19)
- Core Financial Controls: Payroll (5.18/19)

The 22 management actions considered in this review comprised of six 'medium' and sixteen 'low' actions. The focus of this review was to consider if all actions previously made have been adequately implemented.

Conclusion

Taking account of the issues identified in the remainder of the report and in line with our definitions set out in Appendix A, in our opinion Transport for the North has demonstrated **good progress** in implementing agreed management actions.

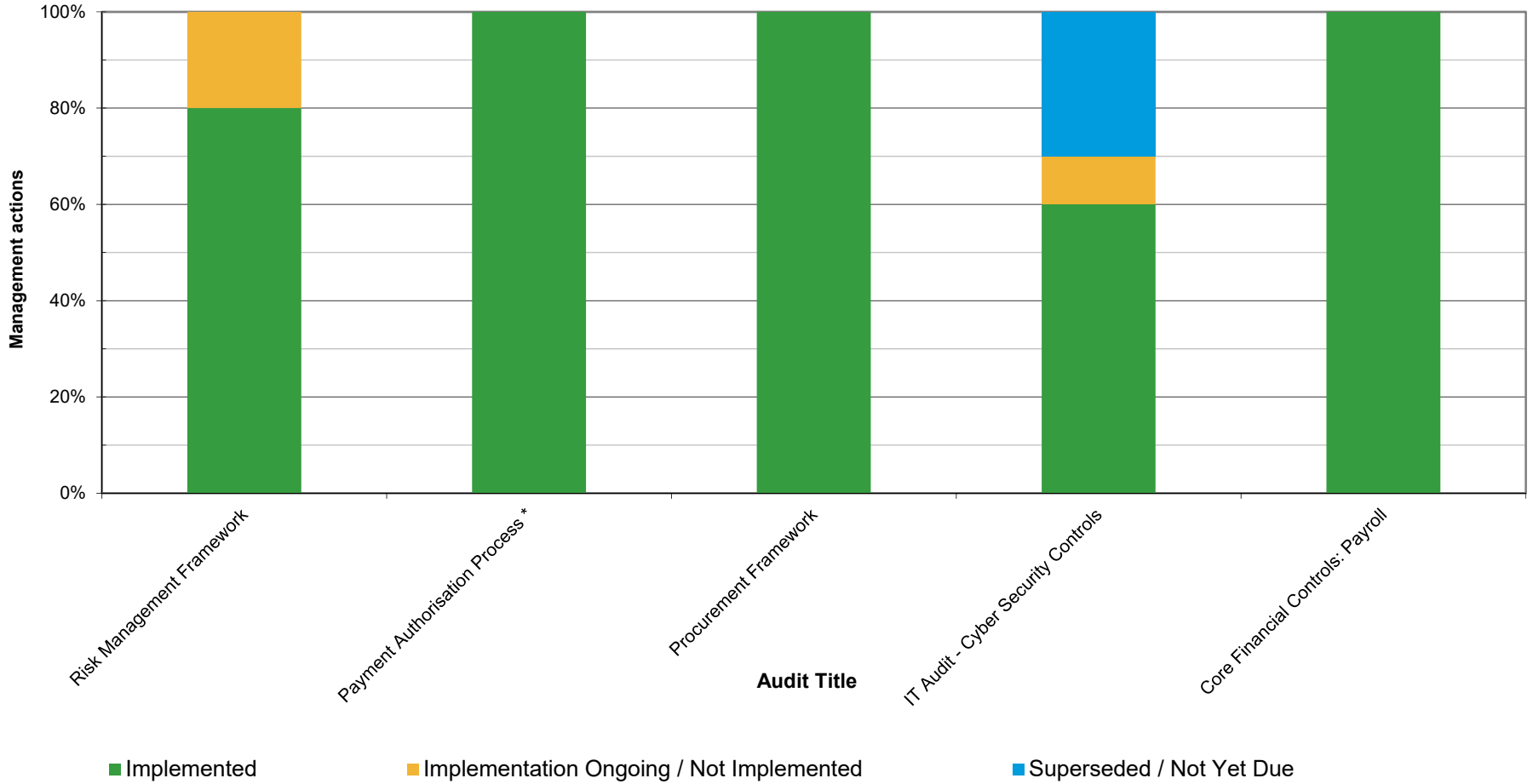
Through testing and discussions with key members of staff we confirmed that 73% of the actions had been implemented, with 9% implementation ongoing, 5% not yet due for implementation and 13% superseded.

We have increased the original priority from low to medium in regards to the cyber training management action, taking into consideration the increased risk of phishing linked to the Covid-19 outbreak for example.

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				
		Impl. (1)	Impl. ongoing (2)	Not impl. (3)	Superseded (4)	Confirmation as completed or no longer necessary (1)+(4)
Risk Management Framework (1.18/19)	5	4	1	0	0	4
Payment Authorisation Processes, Expenses and Use of Procurement (2.18/19)	2	2	0	0	0	2
Procurement Framework (3.18/19)	4	4	0	0	0	4
IT Audit – Cyber Security Controls (4.18/19)	10	6	1	0	3	9
Core Financial Controls: Payroll (5.18/19)	1	1	0	0	0	1
Total	**22**	**17**	**2**	**0**	**3**	**20**



* Payment Authorisation Processes, Expenses and Use of Procurement

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.

Risk Management Framework (1.18/19)				
Original management action / priority	Management will review the value and applicability of the inclusion of a defined assurance framework within each of Transport for the North's risk registers. (Low)			
Audit finding / status	At the time of review the 2020/2021 business planning process cycle was work in progress as planned. Discussions with the Portfolio Risk Manager confirmed that the assurance framework has not yet been adopted by TfN and will be considered as part of the 2020/21 business planning process.			
Management Action 1	Action restated. Management will review the value and applicability of the inclusion of a defined assurance framework within each of Transport for the North's risk registers.	**Responsible Owner:** Leadership Team - Consideration of the assurance framework will be part of the 2020/21 business planning process (drafting starts September 2019)	**Date:** Dependent on the adoption of the TfN Assurance Framework	**Priority:** Low

IT Audit: Cyber Security Controls (4.18/19)				
Original management action / priority	Management will implement mandatory Cyber Security training modules for all staff and monitor compliance rates, to ensure all staff are trained and kept up to date on cyber security best practises on an annual basis. Management should identify additional training needs of staff members deemed to be more critical and/or vulnerable and assign additional training requirements to this group of staff as appropriate. (Low)			
Audit finding / status	We confirmed with the IT Manager that they had not yet implemented mandatory Cyber Security training modules for all staff and therefore at present compliance rates are not monitored. At the time of review the following had been confirmed through email received from the IT Manager: • Greater than 1 year since GDPR & Data Security Training - 65.1% had not been trained; • Greater than 18 months since GDPR & Data Security Training - 0 % of staff require training; and • By the end of March 2020 all staff will have received the mandatory training. We were informed that due to TfN's revised ways of working TfN is moving to an online Cyber Security training module that will become mandatory for all staff to complete. We understand the course has been reviewed by TfN and is suitable for all competency levels and that compliance will be monitored and escalated to line managers where required. Communications regarding this migration is to be provided to all staff in April 2020.Therefore, we consider this action to be ongoing.			
Management Action 2	Action restated. Management will implement mandatory Cyber Security training modules for all staff and monitor compliance rates, to ensure all staff are trained and kept up to date on cyber security best practises on an annual basis. Management should identify additional training needs of staff members deemed to be more critical and/or vulnerable and assign additional training requirements to this group of staff as appropriate.	**Responsible Owner:** Kevin Willans, IT Manager	**Date:** 30 May 2020	**Priority:** Medium

APPENDIX A: DEFINITIONS FOR PROGRESS MADE

Progress in implementing actions	Overall number of actions fully implemented	Consideration of high priority actions	Consideration of medium priority actions	Consideration of low priority actions
Good	75% +	None outstanding.	None outstanding.	All low actions outstanding are in the process of being implemented.
Reasonable	51 – 75%	None outstanding.	75% of medium actions made are in the process of being implemented.	75% of low actions made are in the process of being implemented.
Little	30 – 50%	All high actions outstanding are in the process of being implemented.	50% of medium actions made are in the process of being implemented.	50% of low actions made are in the process of being implemented.
Poor	< 30%	Unsatisfactory progress has been made to implement high priority actions.	Unsatisfactory progress has been made to implement medium actions.	Unsatisfactory progress has been made to implement low actions.

The following opinions are given on the progress made in implementing actions. This opinion relates solely to the implementation of those actions followed up and does not reflect an opinion on the entire control environment.

APPENDIX B: ACTIONS COMPLETED OR SUPERSEDED

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

Assignment title	Management actions and categorisations
Risk Management Framework (1.18/19)	**Implemented** Management will ensure that links to Transport for the North's strategic objectives are explicitly recorded against risks included within Transport for the North's Corporate Risk Register. This may be implemented through the addition of a column to the Corporate Risk Register which outlines how each risk links to the relevant strategic objective. Additionally, management will ensure that updates are included on a periodic basis within the relevant 'Control/ Monitor Stage' column, against each risk included within each risk register. The update shall include a date that the update was added to the risk. Should no update be provided then this shall be recorded for completion purposes. (Low)
Risk Management Framework (1.18/19)	**Implemented** Management should ensure that Mitigation Strategies included within Transport for the North's risk registers are clear and quantifiable controls that can be reliably measured. Management will ensure that the use of 'ongoing' within target date completion columns is minimised. Should the use of 'ongoing' be a necessity, a periodic review timescale shall be stated. (Medium)
Risk Management Framework (1.18/19)	**Implemented** Management will establish 'target' risk ratings against all risks included within the Corporate Risk Register. (Low)
Risk Management Framework (1.18/19)	**Implemented** Management will review the requirement of the production of Quarterly Risk Reports stated within Transport for the North's Risk Management Strategy. This review will cover applicability to Transport for the North's risk management processes and resource available to produce and monitor the Quarterly Risk Reports. (Low)

Assignment title	Management actions and categorisations
Payment Authorisation Processes, Expenses and Use of Procurement Cards (2.18/19)	**Implemented** Staff will be reminded of the Transport for the North's procedure to obtain signed letter headed paper prior to suppliers being set up in the Finance system. (Low)
Payment Authorisation Processes, Expenses and Use of Procurement Cards (2.18/19)	**Implemented** The requirement to submit procurement transaction logs within five working days of month end will be amended in the policy to a more achievable timeframe. (Low)
Procurement Framework (3.18/19)	**Implemented** The Procurement Policy will be uploaded to the Polices section of the Transport for the North's Share Point site. (Low)
Procurement Framework (3.18/19)	**Implemented** The Supplier Recommendation Report will be amended to require staff authorising the procurement of goods and services from a chosen supplier to declare any interests in the supplier. (Medium)
Procurement Framework (3.18/19)	**Implemented** The process flowchart for setting up new suppliers will be updated to include all process carried out in practice, such as the verification of bank details and completion of the bank verification form. The flowchart will also include the required verification checks for processing requests made by suppliers to amend details such as bank details and telephone numbers etc. (Low)
Procurement Framework (3.18/19)	**Implemented** The Contract Log will be updated to include indication of whether contract documentation has been uploaded to Share Point. This information can then be used to monitor and report compliance. (Low)

Assignment title	Management actions and categorisations
	Management Comment It was noted that whilst the Contract Log has been updated to reflect further details, there are currently a number of gaps identified. The Procurement Manager is currently working through these gaps.
IT Audit – Cyber Security Controls (4.18/19)	**Implemented** Management will ensure that resources are assigned, and a completion date is set for completing penetration tests for the external network. Following this, if there are issues identified by the test, an action plan to rectify these should be put in place. (Medium) **Management Comment** We were advised by the Head of IT and Information that the network providers undertook penetration testing at both sites (Manchester and Leeds) and no further were identified as a result of this. An independent exercise will be commissioned during 2020. No evidence in regards to the penetration testing was provided and therefore management assurance was sought in regards to this.
IT Audit – Cyber Security Controls (4.18/19)	**Superseded** Management will ensure that the use of removable media by staff is evaluated; and if considered unnecessary, relevant technical controls will be implemented to disable the connection of such devices on the network. (Medium) **Management response** It was confirmed by the IT Management that Transport for the North has accepted the risk associated with Information Technology systems and services. We were provided with copies of the associated risk acceptance form to confirm this.
IT Audit – Cyber Security Controls (4.18/19)	**Superseded** Management will evaluate the risk of providing all users with Local Administrator access rights on their corporate devices and take appropriate action based on the decision reached. (Medium) **Management response**

Assignment title	Management actions and categorisations
	It was confirmed by the IT Management that Transport for the North has accepted the risk associated with Information Technology systems and services. We were provided with copies of the associated risk acceptance form to confirm this.
IT Audit – Cyber Security Controls (4.18/19)	**Implemented** Management will ensure that the standard build for PCs is updated as per IT security best practices. This will include, ensuring that all devices are up to date with the latest security patches. (Medium)
IT Audit – Cyber Security Controls (4.18/19)	**Implemented** Management will ensure that a patch management policy is documented to outline procedures for patching that are in line with the Transport for the North's risk appetite. (Low)
IT Audit – Cyber Security Controls (4.18/19)	**Implemented** Management will ensure that a formal process is developed for testing patches before they are released to the network, in order to confirm they do not have any unforeseen adverse effects or cause unnecessary service outage. (Low)
IT Audit – Cyber Security Controls (4.18/19)	**Superseded** Management will formally evaluate the risks associated with home and mobile working. (Low) **Management Comment** It was confirmed by the IT Management that Transport for the North has accepted the risk associated with Information Technology systems and services. We were provided with copies of the associated risk acceptance form to confirm this.
IT Audit – Cyber Security Controls (4.18/19)	**Implemented** Management will ensure that clear desk checks are conducted on a regular basis to ensure that staff are adhering to the Office and Desk Protocol. Where required, training and awareness should be provided to staff to ensure compliance with the Protocol.

Assignment title	Management actions and categorisations
	(Low) **Management Comment:** We were advised by the Head of IT and Information that regular checks are completed, and findings fed back at the point of the checks. Due to the nature of the spot checks, no evidence is retained in regards to these.
IT Audit – Cyber Security Controls (4.18/19)	**Implemented** Management will ensure a movers and leavers process is documented to ensure that there is clarity regarding the process, the forms to use and the key people responsible. Once implemented, management should ensure that no user accounts are created, amended or deleted unless the correct process has been followed. (Low)
Core Financial Controls: Payroll (5.18/19)	**Implemented** Management will develop a new user request form to ensure that documented authorisation is obtained for staff granted access to payroll processing module in the Talent system. (Low)

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 manages the following area:

Objective of the area 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 six 'medium', and 16 'low' priority management actions raised in the following assignment reports:

- Risk Management Framework (1.18/19)
- Payment Authorisation Processes, Expenses and Use of Procurement Cards (2.18/19)
- Procurement Framework (3.18/19)
- IT Audit – Cyber Security Controls (4.18/19)
- Core Financial Controls – Payroll (5.18/19)

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;
- Any management actions agreed within the 2019/20 Audit Plan will be followed up as part of next year's work;

- 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; and
- 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.

Debrief held	31 January 2020/ last evidenced request 6 March 2020	**Internal audit Contacts**	Lisa.Randall@rsmuk.com / +44 7730 300309 Alex.Hire@rsmuk.com / +44 7970 641757 Alison.Barlow@rsmuk.com
Draft report issued	18 March 2020		
Responses received	9 April 2020		
Final report issued	9 April 2020		
		Client sponsor	Iain Craven, Finance Director
		Distribution	Iain Craven, Finance Director

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 Transport for the North, 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 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 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 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.