TRANSPORT FOR THE NORTH

Cyber Security Assessment

Internal audit report 6.21/22

Final

16 February 2022

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, or undertake full population testing using data analytics tools, to complete the work in line with the agreed scope.

Why we completed this audit

A cyber security review of Transport for the North (TfN) was undertaken as part of the approved 2021/22 internal audit plan. The objective of the review was to ensure that selected controls are in place to help reduce the risk of cyber related incidents.

This review includes five of the National Cyber Security Council's (NCSC) ten steps. The five steps that we have covered in line with management concerns are:

- Asset Management;
- Data Security;
- Architecture and Configuration;
- Identity and Access Management; and
- Vulnerability Management.

We have not covered the following NCSC steps as part of our review:

- Engagement and Training;
- Risk Management;
- Logging and Monitoring;
- Incident Management; and
- Supply Chain Security.

In the past 18 months, we have seen the cyber-crime threat landscape amplified by the impact of the COVID-19 pandemic as cyber criminals seek to capitalise on the disorder. Our recent 2021 survey highlighted that 20 per cent of organisations had experienced a cyber-attack over a 12 month period, with 71 per cent stating the attack was a direct result of the coronavirus pandemic (https://www.rsmuk.com/real-economy/cybersecurity).

Conclusion

Overall, we identified several missing controls which, when implemented correctly, are designed to protect the information systems network operated by TfN.

This review identified one ‘high’ priority finding which we consider requires immediate management attention. A further two ‘medium’ priority findings and three ‘low’ priority findings have been highlighted.

The high priority finding relates to penetration testing which was previously identified in RSM cyber security review 2019/20, which is yet to be scheduled and performed. Without testing being performed, the full extent of vulnerabilities are not known and a risk-based remediation plan cannot be produced. Given the current cyber control environment, the risk of a successful cyber-attack is significantly increased.

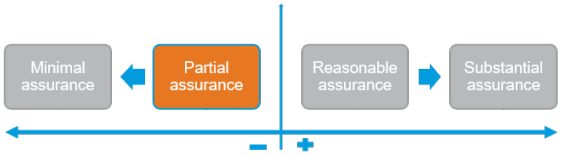
The medium priority findings relate to controls for cyber-incident prevention and include:

- The implementation of Intrusion Detection and Prevention tools in the Manchester office;
- The formalisation of policies and procedures to ensure that controls operate consistently (e.g. a formalised staff onboarding and offboarding procedure); and
- The risk acceptance and mitigation is not reviewed on a periodic basis to ensure this remains within risk appetite.

Internal audit opinion:

Taking account of the issues identified, the Board can take partial assurance that the controls upon which the organisation relies to manage this area 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 areas.



Key findings

We identified the following findings:

Formal penetration testing has never been conducted due to logistical obstacles raised by Covid-19. Without having undertaken penetration tests, the risk of exposure to possible attack is unknown which could lead to data leakage, operational and financial loss and/or reputational harm. As such, a 'high' priority action has been raised (1).

There is no Intrusion Detection and Prevention Service provided by Transport for Greater Manchester (TfGM) on the firewall in the Manchester Office. There is a risk that without a monitoring service enabled, the possibility of a successful cyber-attack is increased. This could cause a loss in productivity and/or reputational harm to TfN. We have raised a 'medium' priority action in light of this finding (2).

Risks are recorded in a risk register however they have not been periodically reviewed. There is a risk that without periodic review of risk acceptance and mitigation, the details of the accepted risks may be outdated, and existing mitigating controls may no longer be applicable or effective. We have raised a 'medium' priority action in light of this finding (3).

Examples of good practice identified during the audit

Autopilot has allowed TfN to improve their hardened configuration and this can be used to build new laptops quickly and consistently. Through review of the standard build specifications, we noted this includes a number of security practices expected such as encryption.

Due to TfN primarily using Infrastructure as a Service (IaaS) and Software as a Service (SaaS) models, and providing their own in-house support, they only need to grant third-parties access to TfN's network infrequently. When access to the TfN network is required, the third-party must submit a request including who will use the user account and before approval is granted by TfN's IT management. The account will be set up with a short expiry date that will depend on what work is to be completed, normally ranging from 24 to 48 hours.

TfN use Microsoft Azure Backup Centre which is a centralised backup solution to help protect against ransomware. Backups are successfully completed daily, with weekly and monthly retention points stored. TfN have the ability to restore backups from a paired region at any time.

TfN has developed a Patching Policy that is up to date, regularly reviewed and our sample based testing showed this was implemented. The policy makes the distinction between security and functional patches, helping to ensure security patches are tested and rolled out more efficiently than would otherwise be possible. We verified that security and functional patches are installed for a selected sample based upon release and were tested on a small number of laptops. Then after 14 days security patches are installed automatically on the IT estate with functionality patches installed after 90 days, unless required sooner.

TfN use Microsoft Azure Information Protection (AIP) which enables them to classify all data stored and processed on SharePoint and to set levels of confidentiality against data. This also allows IT management to track who uses and alters certain data.

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: Network Security				
Missing Control	Penetration testing has been conducted, including a remediation plan and vulnerabilities addressed within timeframes stated in the policy.		**Assessment:** **Design** × **Compliance** N/A	
Findings / Implications	We have noted that in the previous cyber security review, issued in September 2020, penetration testing was recommended to be conducted as a medium priority finding. Management agreed, however these had not been conducted due to other priorities during Covid-19. Formal penetration testing was scheduled for December 2021, but this was postponed by management. All Servers are hosted within the Azure cloud environment are provided by Microsoft. However, without having run penetration tests on the Azure applications as well as the local network firewalls, the risk of exposure to possible attack is unknown to TfN. A cyber-attack could lead to data leakage, operational and financial loss or reputational harm.			
Management Action 1	Management will ensure that penetration testing is conducted as scheduled from week commencing 28 February 2022, the test results are to be reviewed and vulnerabilities addressed and remedied in a timeous manner. Where penetration testing does not go ahead, this will be reported to the relevant TfN governance and oversight groups.	**Responsible Owner:** Head of IT and Information	**Date:** Penetration testing is scheduled to be performed the week commencing 28 February 2022 when staff return to work from the office.	**Priority:** High

Area: Network Security				
Missing Control	Intrusion Detection and Prevention activity is monitored on the network firewalls alerting IT to any possible threats.		**Assessment:** **Design** × **Compliance** N/A	
Findings / Implications	There is no Intrusion Detection and Prevention Service provided by Transport for Greater Manchester (TfGM) on the firewall in the Manchester Office. Combined with the delay in penetration testing being conducted, there is a risk that without monitoring enabled, the risk of a successful attack is increased. This could cause a loss in productivity and/or reputational harm to the organisation.			
Management Action 2	Management will consider implementing Intrusion Detection and Prevention tools to help protect the Manchester office, in line with controls implemented in the Leeds office.	**Responsible Owner:** Head of IT and Information	**Date:** 31 March 2022 – Increase in support service provision to be performed in line with the highlighted management action	**Priority:** Medium

Area: Secure Configuration				
Missing Control	Risks are recorded in a risk register and periodically reviewed.		**Assessment:** **Design** × **Compliance** N/A	
Findings / Implications	We have noted the accepted risks which are captured in the Risk Register and there is an informal requirement that these should be reviewed at least annually. However, the Risk Identification Acceptance Forms provided (Home Agile Working, SharePoint Online Backups, USB Access and User Device Administration) were submitted and approved in November 2019, showing no scheduled review dates.			

	There is a risk that without periodic review of risk acceptance and mitigation, the details of the accepted risks may be outdated, and existing mitigating controls may no longer be applicable or effective. This could result in greater exposure to the risk of a cyber-attack than is within TfN's risk appetite.			
Management Action 3	Management will ensure that the risk register is formally reviewed on a periodic basis, and that version control is applied. Details of the approver as well as the next review date should be included. Reviews should be conducted at least annually to ensure the risk treatment is appropriate given the threats and risks faced.	**Responsible Owner:** Head of IT and Information	**Date:** These risks will be captured immediately in the risk register system called Predict! where alerts for periodic review will be automatically enabled.	**Priority:** Medium

Area: Managing User Privileges			
Missing Control	A formal process has been established for creating and removing access rights for staff members.	**Assessment:**	
		Design	×
		Compliance	N/A
Findings / Implications	Although processes exist, no formal staff and contractor onboarding or offboarding process has been formally documented and agreed. Where starters, movers and leavers processes are not formal and documented, there is an increased risk that user access rights do not reflect their business role and/or are not removed in a timely manner. Through additional conversation with the Head of IT, it was determined that the case in question was an outlier. Requirements for granting of access to information linked to that account, after termination of employment, are not included in the existing process. Stricter controls will be enforced going forwards and this will be communicated to all staff. Further, there is a risk that IT equipment is not appropriately assigned and returned in a timely manner. This could lead to unauthorised access to TfN IT systems and data, as well as unnecessary costs being incurred.		
Management Action 4	Management should define and document a standardised onboarding and offboarding procedure document. This should include, but not be limited to:	**Responsible Owner:** Head of IT and Information	**Date:** 31 March 2022	**Priority:** Low

	• Responsibility for requesting and actioning starter, mover and leaver requests; • Appropriate authorisation of access requests; • Appropriate access to Email and OneDrive data which was linked to the account is granted to an approved manager; • Provision for the immediate removal of access for staff due to disciplinary matters in line with a Service Level Agreement, determining acceptable timelines for various types of leavers; and • An assessment recording the condition of equipment (issued and returned) with an acceptable use policy stating that the responsibility lies with the staff member should items be damaged beyond acceptable standards.			

Area: Network Security				
Missing Control	The firewall forms part of a High Availability pair in order to provide uninterrupted internet connectivity and network redundancy.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	We have noted that there is no backup connectivity in place in the Leeds office. Should the device fail, or suffer an outage from the service provider, this single point of failure increases the risk of downtime and loss in productivity should the connection not be functional. Further, no formal and documented risk acceptance is in place. An additional line is in place in the Manchester office. This primarily allows TfGM to make changes to the Firewall however, we were informed by the Head of IT that they can re-route traffic over this line to provide some redundancy, should the main connection be down. While TfN do have a limited number of 4G backup dongles available in each office, it has been noted that no incoming connectivity to the sites is required as the infrastructure is predominantly cloud based. This allows users to connect from home should the connectivity at the office fail.			
Management Action 5	Management will consider comparing the business case of providing network redundancy against the cost of possible business downtime which may be incurred during a network outage.	**Responsible Owner:** Head of IT and Information	**Date:** 31 March 2022	**Priority:** Low

Area: Managing User Privileges				
Missing Control	Policies are approved by the Board and reviewed annually. Documents are updated with any changes that may be required.		**Assessment:**	
			Design	×
			Compliance	N/A
Findings / Implications	We noted that not all policies are up to date. For example, in the 'ITP04 Security Policy v2.2', the password requirements differ from the actual password policy settings in place (6 characters versus 8 for example). An annual policy review is evidenced, however the policy does not necessarily reflect this. There is a risk that outdated policies may not be in line with good practice. Regular reviews also ensure that policies are up to date with industry standards and technologies.			
Management Action 6	Management should ensure that policies are reviewed on a periodic basis in line with practices across the business. Where a change is required, this should be made on a timely basis and changes communicated to relevant stakeholders.	**Responsible Owner:** Head of IT and Information	**Date:** 31 March 2022	**Priority:** Low

Area: Secure Configuration				
Missing Control	The AutoPlay facility on removable media is disabled by default.		**Assessment:**	
			Design	×
			Compliance	N/A
Findings / Implications	We have noted that the use of removable media is an accepted risk and is documented in the risk register. However, the removable media AutoPlay function is not disabled by default. When enabled, connecting removable media, Windows will detect it, and AutoPlay will launch the media using a default action, which can include the running of potentially malicious executable files. Where USB functionality is allowed and the AutoPlay setting is not disabled, this increases the risk that the network could be breached via means of an intentional placement of a malicious USB device by a staff member. The Head of IT and Information had advised us, after the debrief, that the AutoPlay function is now disabled for all media devices.			
Management Action 7	Management will ensure that the AutoPlay function for removable media is disabled by default on all devices.	**Responsible Owner:** Head of IT and Information	**Date:** Completed 31 January 2022	**Priority:** Observation

	Evidence received from the Head of IT and Information on 31 January 2022 showing that the AutoPlay function has now been disabled by default for all devices.

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
Failure to manage cyber risks effectively could lead to the loss of systems confidentiality and availability, together with a potential financial impact including fines or other penalties for breach of statutory obligations such as data protection.	6	(18)	0	(18)	3	2	1
Total					**3**	**2**	**1**

* 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 internal audit assignment has been scoped to provide assurance on how Transport for the North (TfN) manages the following risks.

Objective of the risk under review	Risks relevant to the scope of the review	Risk source
To review select cyber security controls to ensure computer systems and data are resilient to threats resulting from connection to the internet.	Failure to manage cyber risks effectively could lead to the loss of systems confidentiality and availability, together with a potential financial impact including fines or other penalties for breach of statutory obligations such as data protection.	Internal Audit

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

The Audit Committee and management have requested this audit to examine how TfN manages cyber risk. The areas set out in this audit

The following areas will be considered as part of the review:

Secure Configuration

An assessment of the high-level controls focussing on:

- Patching of user endpoints and third-party software.
- Standard build of user devices.

Malware Protection

An assessment of the high-level controls focussing on:

- Use and upkeep of anti-virus software.

Network Security

An assessment of the high-level controls focussing on:

- Firewall rules and settings (including Intrusion Detection and Prevention System(s)).
- Penetration testing and vulnerability management.

Managing User Privileges

An assessment of the high-level controls focussing on:

- Process for user account creation, deletion and amendment.
- Password rules for end user and administrative accounts.
- Rules around remote and third-party access to network.

IT Resilience and Disaster Recovery

An assessment of the high-level controls focussing on:

- Backup schedules and testing.
- IT Disaster Recovery Plan and restore procedures.

Limitations to the scope of the audit assignment:

- The scope of our work will be limited only to those areas that have been examined and reported and is not to be considered as a comprehensive review of all aspects of Cyber Security Risk.
- This audit will not review areas related to cyber security such as risk management, mobile working, user education, incident management or monitoring.
- The approach taken for this review will be to validate the design and testing of key controls.
- We will be testing key controls on a sample basis and for the financial year only.
- We will not perform penetration tests and vulnerability assessments however we will review the results of tests undertaken by independent service providers.
- The information provided in the final report should not be considered to detail all errors or risks that may currently or in the future exist within the cyber security environment, and it will be necessary for management to consider the results and make their own judgement on the risks affecting TfN and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised.
- In addition, our work does not provide an absolute assurance that material error; loss or fraud does not exist.

Debrief held	24 January 2022 and 8 February 2022	**Internal audit Contacts**	Lisa Randall, Head of Internal Audit (IA) Alex Hire, IA Senior Manager Andrew Mawdsley, IA Assistant Manager Paul O'Leary, Technology Risk Assurance (TRA) Lead Wil Milligan, TRA Senior Consultant Martin Kagho, TRA Consultant Graeme Clarke, TRA Consultant
Draft report issued	7 February 2022		
Responses received	7 and 15 February 2022		
Revised Draft report issued	15 February 2022		
Final report issued	16 February 2022	**Client sponsor** **Distribution**	Iain Craven, Finance Director Kevin Willans, Head of IT and Information Iain Craven, Finance Director

rsmuk.com