TRANSPORT FOR THE NORTH

Cyber Security Review

Internal audit report 5.20/21

Final

5 November 2020

1. EXECUTIVE SUMMARY

With the use of secure portals for the transfer of information, and through electronic communication means, remote working has meant that we have been able to complete our audit and provide you with the assurances you require. It is these exceptional circumstances which mean that 100 per cent of our audit has been conducted remotely. Based on the information provided by you, we have been able to undertake sample testing.

Why we completed this audit

An audit of Transport for the North's (TfN) cyber security control environment was undertaken as part of the annual internal audit plan. The audit assessed the technology, governance and processes control framework designed to protect TfN's computers, systems and data from attack, damage or unauthorised access.

With technology becoming increasingly integrated within the processes of all organisations, it is important to consider the risks it presents to the processes themselves, the protection of organisational assets and information, and to the people the organisation serves. Additionally, given the legal requirements of the General Data Protection Regulation (GDPR), the importance of data security has become an important focus for many organisations. Ensuring strong cyber security controls are in place will help to minimise the risk of personal data breaches for which the Information Commissioner's Office (ICO) can impose severe penalties under GDPR.

This is particularly relevant for TfN who have established an entirely cloud based network in Azure. TfN operate primarily on Infrastructure as a Service (IaaS) and a Software as a Service (SaaS) cloud models. Whilst this does help to streamline the IT department and the services it offers, it poses its own, new challenges where security risks are heightened over traditional servers due to the potential for an attack or a compromised hypervisor to gain access to key infrastructure services.

The audit was primarily carried out through sample-based testing, meetings with the Head of IT and Information and the IT Security and Data Compliance Officer and the review of key documentation.

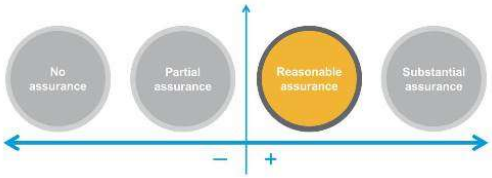
Conclusion

Our review has highlighted positive areas of good practice and some controls that are missing or require enhancing. TfN has established regular steering group meetings to review the Risk Management Strategy and implemented some strong technical controls to help maintain a secure IT environment. However, the controls requiring enhancement or that are missing include controls over user access, reviews of permissions, external vulnerability testing, policy review and Business Continuity and IT Disaster Recovery planning and testing. A number of control improvements are required to enhance TfN's cyber security controls. Two medium and two low priority management actions have been raised in order to strengthen the control environment.

Internal audit opinion:

Taking account of the issues identified, the Board can take reasonable assurance that the controls in place to manage this risk are suitably designed and consistently applied.

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.



Key findings

We identified the following key findings:

There are a number of contractors whose user accounts are not being deactivated when they leave TfN. Their user accounts remain active for days and sometimes weeks after they have ceased to work for TfN. Given TfN's SharePoint site can be accessed from any personal device, this issue increases the risk of unauthorised access of sensitive data. Additionally, there are no periodic reviews of user access and permissions to ensure it remains up to date.

TfN has not conducted a penetration test for over 18 months. Given the fast-changing nature of cyber risks, it is important that a penetration test is conducted at least annually. Not doing increases the risk of TfN not being aware of vulnerabilities to the IT network making them susceptible to a cyber-attack.

Good Practice

We identified the following areas of good practice:

The IT risk register is reviewed quarterly as part of the IT and Facilities Steering Group and the Risk Management Strategy is reviewed annually by the Risk Manager and approved by the Audit and Risk Committee. Additionally, TfN use risk acceptance forms, which provide detail on the risk description (risk, root cause, impact), risk owner, mitigation action owner and mitigating actions. We were informed accepted risks are to be reviewed by the IT and Facilities Steering Group or on an ad hoc basis should the security environment change as new threats emerge.

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

TfN has developed a Patching Policy that is up to date, regularly reviewed and subject to testing was shown to be compliant in practice. The policy makes the distinction between security and functionality patches, helping to ensure security patches are tested and rolled out more quickly. We verified that patching is configured such that security and functionality patches are installed as the patches are released to be tested on a small number of laptops. Then after 14 days security patches are installed automatically on the IT estate and functionality patches after 120 days, unless required sooner.

There are a variety of different security applications in use. These include Windows Defender which provides anti-virus, a personal firewall and Intrusion Detection System (IDS) and spam filters. This is positioned alongside a proxy server for each laptop and added anti-virus and spam protection provided by Azure that is present on SharePoint.

Due to TfN primarily operating off Infrastructure as a Service (IaaS) and Software as a Service (SaaS) models they rarely have to grant third-parties access to TfN's network. When they do the user at the third-party must submit a request including who will use the user account and then gain approval from TfN's IT management. The account will be set with a short expiry date that will depend on what work is to be completed, normally ranging from 24 to 48 hours.

TfN use Azure Information Protection (AIP) which enables them to classify all data stored and processed on SharePoint and to set levels of confidentiality against data. It also allows IT management to track who uses and alters 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: Managing User Privileges				
Control	There is a leavers procedure for the submission of leavers requests to IT for contractors and permanent staff. In particular, TfN has implemented a process for leavers whereby HR update their 'TALENT' records and submit a leaver request to the Service Desk. However, there is no policy or procedure to ensure periodic review of user access permissions.	**Assessment**	**Design**	×
			Compliance	N/A
Findings / Implications	Our testing identified a number of leaver requests for contractors that were submitted over three and four months after the individuals had ceased working for TfN. For the sample we tested, we noted when a leaver request is submitted to IT, it was actioned straight away, and their user access removed. We found that the delay in the submission of leavers requests had not affected permanent TfN employees, just contractors. By not submitting a leaver request to IT via the Service Desk, contractors login details are not being deactivated and they can access TfN's SharePoint site. The SharePoint site can be accessed from a personal device meaning that the contractor will have read access to TfN's applications and data despite their contract having ended as permissions are all managed through SharePoint. This significantly increases the risk of non-compliance with GDPR and potential data breaches. We noted that contractors are employed by a third-party with which TfN has an ongoing non-disclosure agreement in place. However, the risk of unauthorised access remains as the contractors could still have access to TfN's systems and data. Through discussion with the Head of IT and Information we were informed that SharePoint owners are responsible for reviewing permissions and access to their folders on SharePoint. However, there is no formal control to ensure that this review is taking place on a continuous or periodic basis. This increases the risk that inappropriate access rights are not removed when an employee changes role within TfN. In addition, there is the risk that that staff may not have appropriate permissions for their role. We were informed by the Head of IT and Information that there was an ad hoc review of access permissions at the start of 2020 (January 2020) which identified a leaver that had not been processed correctly and retained system access. This was not followed up with implementing the same review on a periodic basis.			
Management Action 1	Management will review the current leavers process for employees and contractors and ensure that leaver forms are approved and submitted in a timely manner to enable their system access to be revoked.	**Management Comment:** Leaver process to be reiterated to all line managers with additional focus to be placed on those with contractors in site.	**Date:** 31 October 2020	**Priority:** Medium

	Management will review the leavers procedure and document that a leavers request needs to be submitted to IT prior to that individual leaving TfN. This will clearly state the responsibilities of the stakeholders in the leavers process to ensure the timely submission of leavers requests. Management will also establish a periodic review control to identify users with access to SharePoint who are no longer employed or contracted by TfN, or whose roles and approval for access may have changed within TfN.	SharePoint Access review to be established as a quarterly process confirming site ownership, access levels granted and who has access. **Responsible Owner:** Head of IT and Information		

Area: Network Security			**Assessment**	
Control	There is no formal policy in place that sets out the requirement for an independent, external penetration test to completed on a periodic basis.		**Design**	×
			Compliance	N/A
Findings / Implications	The Head of IT and Information informed us that TfN last undertook an independent penetration test 18 months ago. We were informed the budget had been set aside for the planned penetration test. However, we were informed by the Head of IT and Information that this has not yet been conducted due to TfN being unable to allow safe site access to their Manchester and Leeds offices. It is good practice to undertake penetration tests on an annual basis, or when significant changes are applied to the network components and to rotate the vendors performing penetration tests. This should be followed up with the completion and monitoring of a remediation plan to address the weaknesses identified. In failing to undertake a penetration test, TfN increases the risk that there are vulnerabilities within the network security environment that they are unaware of, making the network more susceptible to a data breach or cyber-attack.			
Management Action 2	Management will ensure an independent penetration test is planned, scoped and conducted. This will be accompanied by a written policy stating how often an independent penetration test should be conducted and in what timeframe vulnerabilities of differing severity need to be addressed. Following this, a remedial action plan will be completed to plan and monitor the implementation of actions required to remediate any identified weaknesses. Priority should be given to address any critical or high vulnerabilities.	**Management Comment:** Budget had been set aside for the penetration test; however, this has not yet been conducted due to logistical obstacles raised by Covid-19. Once safe site access can be established formal penetration tests of both Manchester and Leeds will commence. **Responsible Owner:** Head of IT and Information	**Date:** TBC depending on return to site access	**Priority:** Medium

Area: Information Risk Management				
Control	A number of IT policies and procedures are in place designed to provide governance for IT activities such as the: Information Technology (IT) Policy, the Data Protection Policy, the Security Policy and the Social Media Policy. Some IT policies and procedures contain an incomplete version control whereas others do not, nor do they state how often the policies are to be reviewed.		**Design** **Compliance**	× N/A
Findings / Implications	Upon review of the IT Policy we found that it was up to date, having last been revised on 24 January 2020. We noted that the contents of the policy covered areas such as personal use and responsibility, system access, internet access, use of social media and data protection amongst others. However, the IT Policy did not have clear version control, stating the policy review and approval process and timescale. This increases the risk that the policies or procedures, such as the IT Policy, Information Security Policy and Data Protection Policy, may be outdated and do not reflect the current practices expected to operate on TfN's IT network. We were informed by the Head of IT and Information that staff are required to formally acknowledge the organisation's policies and procedures at their induction. However, we were unable to validate this with evidence from the HR team. In not formally acknowledging the IT Policy staff may be unaware that their actions are endangering TfN's systems and sensitive data, thus increasing the risk of a data breach. Additionally, by not updating existing staff with the revised version of the IT Policy it would be hard to hold them to account for a breach of the policy.			
Management Action 3	Management will ensure all policies and procedures contain the following details for version control: • Date of approval and who by; • Date of most recent and next review and who by; and • Version control to track any changes. Management will also ensure that all staff have read the IT Policy and have agreed to work according to it and are made aware of any updates to it.	**Management Comment:** All IT Policies are to be reviewed an updated in line with the recommendation. **Responsible Owner:** Head of IT and Information	**Date:** 31 October 2020	**Priority:** Low

Area: Business Continuity and Disaster Recovery				Assessment	
Control	There is no complete and signed-off Disaster Recovery or Business Continuity Plan: • Not all Business Impact Assessments (BIA) have been completed and some will now be out of date; • Critical systems have not been put in order of criticality; and • Contact details for staff or third-parties are not included.			**Design** **Compliance**	× N/A
Findings / Implications	The Disaster Recovery and Business Continuity Plan for TfN was initially drafted in July 2018. Whilst the plans have been through several iterative updates since, the last being 3 March 2020, they are still not complete or approved and require the completion of key information such as the results of business impact assessments and recovery procedures. This increases the risk that TfN would not be able to react effectively in the event of a disaster which could lead to a loss of operations and data. However, to provide a level of mitigation, TfN only operate a small number of non-critical systems such as the HR system Nitro. Based on the latest BIA the maximum tolerable downtime of this system was 7 days. This shows that should TfN suffer a disaster they have a full week to recover Nitro. The majority of services are cloud based, operated on a Software as a Service (SaaS) or Infrastructure as a Service (IaaS) model. TfN's network is primarily based on SharePoint, in Azure. TfN's network is replicated across two different Azure datacentres, Azure South and West. We have also obtained certification demonstrating the cloud provider's business continuity capabilities including ISO 9001 and ISO 22301. This has been reflected in the priority of our management action.				
Management Action 4	Management will assign resources for the completion of the Disaster Recovery and Business Continuity Plan. The wider business will be consulted with, a test plan formulated and formally approved. Where systems are hosted by a third party, management will include disaster recovery procedures in the contract and document them in TfN's disaster recovery plan.	**Management Comment:** BCP to be fully reviewed in light of Covid-19 enforced remote working and new Ways of Working principles to be shortly introduced within TfN. As per the draft plan formal testing will then commence once return to site access is possible. **Responsible Owner:** Head of IT and Information	**Date:** 30 November 2020	**Priority:** Low	

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.	4	(28)	0	(28)	2	2	0
Total					**2**	**2**	**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

1.1 Objectives relevant to the scope of the review

Objective of the review	Risks relevant to the scope of the review
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.

1.2 Additional management concerns

Management had requested as part of the annual audit plan that the following IT controls are reviewed:

- IT security policies and procedures;
- Network User registration / De-registration procedures for staff;
- The Password policy is in place and user account security settings governing access to the TFN network;
- System backups; and
- Virus protection software.

1.3 Scope of the review

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

The remit of the review will include an evaluation of a sample of the ten control areas that have been identified by the National Cyber Security Centre of UK Government (formerly Communications Electronics Security Group (CESG) as key control areas for cyber risk management. These are:

Information Risk Management

- Completion of any risk assessments or business impact assessments.
- Senior management oversight of and responsibility for Information/ Cyber Risk Management.

Secure Configuration

- Policies and procedures in in place for the application of security patches applied to software or network devices.
- Standard build of PCs.
- Restrictions on use of removable media.

Malware Protection

- Use and upkeep of anti-virus software.
- Use of file scanning.

Network Security

- Policy on the management of the firewall rules and settings.
- Intrusion detection and prevention.
- Security over physical access to core IT infrastructure (servers and cabling).

Home and Mobile Working

- Inspection of remote working approvals for employees working remotely.
- The relevant policies and procedures regarding home and mobile working.
- The methods and security measures in place for staff who connect remotely into the network.

User Education and Awareness

- User education and awareness in respect of cyber risk.

Incident Management

- Documented incident management procedures including.
- Detection of security breaches or unauthorised access attempts.
- Investigation, escalation and including lessons learned.

Managing User Privileges

- Process for user account creation, deletion and amendment.
- Process for approving user account security settings governing access to the TfN network.
- How access rights are defined and authorised for different individuals.
- Restrictions on access to administrative accounts.
- Password rules for end user and administrative accounts.
- Monitoring of user access.
- Rules around remote and third-party access to network.

Removable Media Controls

- Inspection of policies and procedures for the use of removable media.
- The technical controls in place around the security of removable media.

Monitoring

- The monitoring and reporting processes in respect of incidents and near misses (including successful and unsuccessful attempts to access data).
- Whether monitoring solutions have been put in place to continuously monitor inbound and outbound traffic.

The following limitations apply to the scope of our work:

- The results of our work are reliant on the quality and completeness of the information provided to us.
- 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.
- The approach taken for this review will be to validate the design of controls and will not include all monitoring controls.
- We will be testing key controls and on a sample basis and for the financial year 2020-2021 only.
- 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 Transport for the North and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised.

Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

Debrief held	9 September 2020
Draft report issued	29 September 2020
Responses received	5 November 2020
Final report issued	5 November 2020

Internal audit Contacts	Lisa Randall, Head of Internal Audit (IA) Alex Hire, Client Manager Andrew Mawdsley, IA Assistant Manager John Bradshaw, Technology Risk Assurance (TRA) Managing Consultant Munibah Ahmed, TRA Consultant Wil Milligan, TRA Consultant
Client sponsor	Iain Craven, Finance Director Kevin Willans, Head of IT and Information
Distribution	Iain Craven, Finance Director Kevin Willans, Head of IT and Information

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.