# TRANSPORT FOR THE NORTH

## IT Audit - Cyber Security Controls

### FINAL

### Internal audit report: 4.18/19

### 4 June 2019



RSM

# CONTENTS



| | | | |
|---|---|---|---|
| **Debrief held** | 24 January 2019 | **Internal audit team** | Lisa Randall, Head of Internal Audit<br>Sarah Massel, Assistant Manager<br>David Morris, Technology Risk Director<br>John Bradshaw, Technology Risk Manager<br>Dom Hamilton, Technology Risk Consultant |
| **Draft report issued** | 6 February 2019 | | |
| **Responses received** | 4 June 2019 | | |
| **Final report issued** | 4 June 2019 | **Client sponsor** | Iain Craven, Finance Director<br>Kevin Willans, Head of IT and Information |
| | | **Distribution** | Iain Craven, Finance Director |

# 1 EXECUTIVE SUMMARY

## 1.1 Background

An audit of Transport for the North's ('TfN')'s cyber security controls was undertaken as part of the approved internal audit plan for 2018/19. The objective of the review was to provide assurance over TfN's control framework for managing cyber security risks to ensure TfN's resilience to potential security threats.

The audit was carried out primarily through meetings with key staff - including the Head of IT and Information and the IT Security & Data Compliance Officer - along with a review of key documentation relevant to the scope.

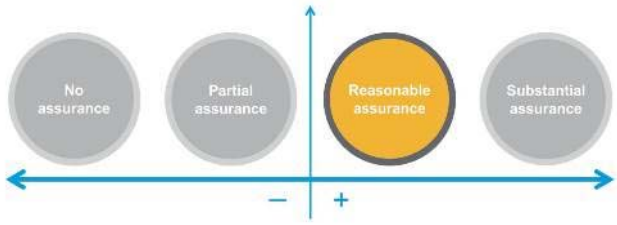
Given the change in data protection legislation, from the Data Protection Act 1998 to the General Data Protection Regulation ('GDPR'), the importance of data security has become a focus for many organisations. As the penalties for breaches of personal data have become far more severe, avoiding vulnerabilities within TfN's cyber security will help to minimise the risks of such breaches.

TfN's core IT operations is heavily cloud based through Azure and Office365, meaning TfN does not maintain much IT equipment onsite and therefore does not have any servers.

## 1.2 Conclusion

TfN has implemented a number of technical controls in order to secure its network against external attackers. However, some control developments are required to further enhance the cyber security control framework. Four medium and six low priority management actions have therefore been proposed within this report.

**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 risks.




## 1.3 Key findings

The key findings from this review are as follows:

- The Head of IT and Information informed us that TfN does not undertake any external penetration testing of its perimeter network. Therefore, there is a risk that management are not aware of vulnerabilities within the network security environment and thus the organisation may be more susceptible to a data breach or cyber-attack.
- TfN does not have a formally documented patch management procedure. Therefore, there is a risk that PCs are not kept up to date, causing known IT infrastructure vulnerabilities to be exploited.
- Windows security and critical updates are not tested prior to being deployed on TfN's machines. There is a risk that a Windows patch may have an adverse effect, which could be detrimental to the IT infrastructure and may lead to service outage.

- All users are currently set up as local administrators on their PCs and laptops. Furthermore, discussion with the Head of IT and Information confirmed that security risks associated with local administrator access has not been formally assessed. There is a risk that users have an inappropriate level of access to privileges on their devices and can install applications or perform actions which create vulnerabilities for the network.

- We noted that there are no restrictions placed upon staff's use of removable media, such as preventing unencrypted removable media devices on its network. Therefore, staff are able to access and copy data onto removable media which has not been encrypted or password protected. This increases the risk that an individual can remove data from the network, which can then easily be recovered by an unauthorised individual if the media is lost or stolen.

- TfN does not undertake periodic clear desk checks to confirm that staff are adhering to the Office and Desk Protocol. Therefore, there is a risk that unauthorised individuals could obtain sensitive information, for example, if left on desks.

- TfN's home and mobile working arrangements are captured within the organisation's "ITP01 IT Policy". However, in discussion with the Head of IT and Information we were informed that the security risks associated with home and mobile working have not been formally assessed. Therefore, there is a risk that TfN has not comprehensively considered all of the risks it faces in its IT environment in relation to home and mobile working by staff.

- Transport for Greater Manchester (TFGM), TfN's IT third party support provider, are responsible for enforcing the standard image build for PCs and workstations across TfN's estate, this includes ensuring that all the PCs and workstations are up to date with the latest security patches. Audit testing confirmed that there were six devices across TfN's estate which were not up to date with the latest security patches. This increases the risk that known network vulnerabilities could be exploited.

- Although staff are made aware of cyber risks and threats through meetings and occasional presentations by members of the IT team, they are not required to complete any formal annual information security or cyber training to keep them up to date with the people risks facing the TfN.

- Audit testing of the starters, movers and leavers did not note any issues with the creation and amendment of users account privileges and the disabling of users' accounts. However, whilst we were able to obtain a completed form for starters, as part of the audit testing for assessing the starters, movers and leavers process, we were not able to obtain an audit trail by the way of a completed form for movers and leavers. Therefore, there is a risk that TfN is unable to provide assurances that the information about movers and leavers has been effectively communicated and acted upon.

  TfN has a formally documented starters process. However, we noted that TfN does not have a formally documented movers and leavers process. This increases the risk that procedures are not being completed in a consistent manner, which may lead to a user account being created with inappropriate permissions, or an account not being disabled in a timely manner.

## 1.4 Additional information to support our conclusion

The following table highlights the number and categories of management actions made. The detailed findings section lists the specific actions agreed with management to implement.

| Risk | Control design not effective | Non Compliance with controls | Agreed actions | | |
|---|---|---|---|---|---|
| | | | Low | Medium | High |
| Loss of information, risks from inappropriate and malicious access, viruses and malware leading to data leakage, financial loss and/or litigation. | 6 | 4 | 6 | 4 | 0 |
| **Total** | | | **6** | **4** | **0** |

Benchmarking

Our overall impression of TfN's culture, with regards to cyber security risk management, was a positive one. The IT team are forward looking and aware of the potential impacts of cyber security risks. This is apparent in their recent and planned IT projects, which include the implementation of Azure and Office365. TfN is aware that its governance of cyber security risks has not fully caught up with its rapid growth and digital transformation as an organisation and recognises the need to develop and improve.

Throughout the review, management demonstrated high-levels of engagement and were proactive in providing information and documentation requested to support the audit testing. Management were also receptive to discussing the points raised by RSM at the debrief stage of this audit. Receptiveness to the improvement of controls was also apparent throughout the IT team, who have the capability to take positive meaningful action on the recommendations made within this report.

In light of this report, we recommend that management assess the impact on TfN's risk profile and, where applicable, update policies, procedural, and risk management documentation to reflect the control enhancements identified.

We have included some comparative data to benchmark the number of management actions agreed, as shown in the table below. In the past year, we have undertaken a number of audits of a similar nature in the sector.

| Level of assurance | Percentage of reviews | Results of the audit |
|---|---|---|
| Substantial assurance | 17.65% | - |
| Reasonable assurance | 47.06% | ✓ |
| Partial assurance | 23.53% | - |
| No assurance | 11.76% | - |
| **Management actions** | **Average number in similar audits** | **Number in this audit** |
| | 7.96 | 10 |

The benchmarking data demonstrates that, in terms of the level of assurance provided, TfN is performing broadly in line with other organisations in our client base where we have carried out similar reviews in the last year. However, a slightly higher than average number of management actions are required as a result of the work undertaken.

# 2 DETAILED 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 regulatory scrutiny/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, regulatory scrutiny, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines. |

This report has been prepared by exception. Therefore, we have included in this section, only those risks of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

| Ref | Control | Adequate control design (yes/no) | Controls complied with (yes/no) | Audit findings and implications | Priority | Action for management | Implementation date | Responsible owner |
|---|---|---|---|---|---|---|---|---|
| **Risk: Loss of information, risks from inappropriate and malicious access, viruses and malware leading to data leakage, financial loss and/or litigation.** | | | | | | | | |
| 2.1 | TfN does not undertake external penetration testing. In addition, TfN does not have a formal policy over the requirements to undertake vulnerability assessments on a periodic basis. | No | N/A | In discussion with management we were advised that independent third-party external penetration tests to identify any vulnerabilities within the network security environment have not been undertaken.<br><br>In addition, there is no formal policy in place outlining the business' approach to penetration testing of its network including the frequency, process for deploying a service provider and applying corrective fixes following the completion of the tests. A security best practice is to undertake these tests on an annual | Medium | 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. | Q1 of 2019/20 | Kevin Willans, IT Manager |

| Ref | Control | Adequate control design (yes/no) | Controls complied with (yes/no) | Audit findings and implications | Priority | Action for management | Implementation date | Responsible owner |
|---|---|---|---|---|---|---|---|---|
| | | | | basis, or when significant changes are applied to the network components such as the firewall.<br><br>Another security best practice to consider is to rotate the vendors performing penetration tests.<br><br>There is a risk that TfN is not aware of vulnerabilities within the network security environment, and thus may be more susceptible to a data breach or cyber-attack. | | | | |
| 2.2 | TfN allows the use of unencrypted removable media devices on its network. | No | N/A | TfN currently allows all staff to use removable media on corporate PCs and laptops. Furthermore, in discussion with the Head of IT and Information we were advised that controls have not been implemented to ensure that all removable media devices are encrypted. Therefore, there is a risk of unauthorised access to data or data loss if data is being stored on unencrypted removable media devices and these become misplaced or stolen. The risk is heightened given the fact that removable media is not required to be encrypted before being used on the network. | Medium | 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. | Completed (June 2019) | Kevin Willans, IT Manager |
| 2.3 | All users are currently set up as Local | No | N/A | Transport for Greater Manchester (TFGM), TfN's IT third party support provider are responsible for configuring each PC to the needs of | Medium | Management will evaluate the risk of providing all users with Local Administrator | Completed (June 2019) | Kevin Willans, IT Manager |

| Ref | Control | Adequate control design (yes/no) | Controls complied with (yes/no) | Audit findings and implications | Priority | Action for management | Implementation date | Responsible owner |
|---|---|---|---|---|---|---|---|---|
| | Administrators on their PCs and laptops. | | | the user. At present, all staff are set up as Local Administrator users on their devices. This gives them the ability to download unauthorised hardware and software; and potentially install or remove software. Discussion with the Head of IT and Information confirmed that security risks associated with Local Administrator access has not been formally assessed.<br><br>There is a risk that users have an inappropriate level of access to privileges on their devices and can install applications or perform actions which create vulnerabilities for the network. | | access rights on their corporate devices and take appropriate action based on the decision reached. | | |
| 2.4 | A standard PC build has been implemented at TfN.<br><br>TfN's third party support provider, Transport for Greater Manchester (TFGM) is responsible for enforcing the image build. The image is installed using the user's credentials as administrators on the device. TFGM update the image quarterly and ensure that the patch | Yes | No | TFGM is responsible for enforcing the standard build for PCs across TfN's estate, this includes ensuring that all the devices are up to date with the latest security patches. Through review of the 'Intune Windows Device Version' spreadsheet provided by management showing the version and patching status, we confirmed that six devices were not up to date with the latest security patches. With devices not being up to date with the latest security patches, this increases the risk that known | Medium | 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. | Completed (June 2019) | Kevin Willans, IT Manager |

| Ref | Control | Adequate control design (yes/no) | Controls complied with (yes/no) | Audit findings and implications | Priority | Action for management | Implementation date | Responsible owner |
|---|---|---|---|---|---|---|---|---|
| | policy from Intune is initiated. | | | network vulnerabilities could be exploited. | | | | |
| 2.5 | TfN does not have a formally documented patch management policy. | No | N/A | Discussion with management confirmed that TfN does not have a formally documented patch management policy in place. In the absence of a formally documented patch management policy, there is a risk that PCs are not kept up to date, causing known network vulnerabilities to be exploited. | Low | Management will ensure that a patch management policy is documented to outline procedures for patching that are in line with the TfN's risk appetite. | 31 March 2019 | Kevin Willans, IT Manager |
| 2.6 | Patches are not tested for unforeseen adverse effects before being deployed to the network. | No | N/A | We confirmed that Microsoft Intune is used for installing and managing patches. We noted that critical and security updates are automatically downloaded and installed onto machines, without first being tested to ensure that there are no unforeseen adverse effects.<br><br>Whilst management informed us that no issues have yet occurred from the lack of patch testing, it is not an indication that no issues will occur in the future and therefore there is a risk that an update can cause a failure, leading to unnecessary IT service outage. | Low | 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. | On-going (quarterly) | Kevin Willans, IT Manager |

| Ref | Control | Adequate control design (yes/no) | Controls complied with (yes/no) | Audit findings and implications | Priority | Action for management | Implementation date | Responsible owner |
|---|---|---|---|---|---|---|---|---|
| 2.7 | TfN's home and mobile working arrangements are captured within the organisation's "ITP01 IT Policy". | Yes | No | TfN's home and mobile working arrangements are captured within the organisation's "ITP01 IT Policy". However, in discussion with the Head of IT and Information we were informed that the security risks associated with home and mobile working have not been formally assessed. Therefore, there is a risk that TfN has not comprehensively considered all of the risks it faces in its IT environment in relation to home and mobile working, and thus potentially has not adequately remediated any high-priority risks to an appropriate level. | Low | Management will formally evaluate the risks associated with home and mobile working. | Completed (June 2019) | Kevin Willans, IT Manager |
| 2.8 | On a quarterly basis phishing exercises are conducted with a view to determine the vulnerability level of the network, by giving TfN an indication of how many people may be susceptible to an email-born social engineering attack.<br><br>Staff at TfN are not currently required to complete any annual cyber security training courses or modules. | No | N/A | TfN has deployed the online tool Kallidus to provide training modules to staff. The software includes training modules for Cyber Security and Data Protection for assessing staff's level of understanding. Staff are required to complete the online Data Protection and GDPR training modules and are given awareness of cyber risks through meetings and occasional presentations by the Head of IT and Information.<br><br>Discussion with the Head of IT and Information confirmed that staff are not required to complete any annual online cyber security training to keep them up to date with the risks facing TfN. Therefore, there is a risk that | Low | 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.<br><br>Management should identify additional training needs of staff members deemed to be more critical and/or vulnerable and assign additional training requirements to | Quarter 1 2019/20 and ongoing | Kevin Willans, IT Manager |

| Ref | Control | Adequate control design (yes/no) | Controls complied with (yes/no) | Audit findings and implications | Priority | Action for management | Implementation date | Responsible owner |
|---|---|---|---|---|---|---|---|---|
| | | | | staff at TfN are not aware of key cyber security threats facing the organisation and therefore are not appropriately trained on how to mitigate these risks. | | this group of staff as appropriate. | | |
| 2.9 | TfN has a clear desk policy in place 'Office and Desk Protocol, which applies to all employees. | Yes | No | In discussion with Management we were informed that TfN does not undertake periodic clear desk checks to confirm that staff are adhering to the Office and Desk Protocol. Therefore, there is a risk that unauthorised individuals could obtain sensitive information, for example, if left on desks. | Low | 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. | Completed (June 2019) | Kevin Willans, IT Manager |
| 2.10 | Role based access configuration is in place to ensure that employees have access rights only to the information they need to do their jobs and prevents them from accessing information that does not pertain to them. | Yes | No | We performed testing on a sample of five new starters to establish whether they had a completed and signed new starter form and had been set up with the correct privileges as per their job roles. No issues were noted.<br><br>We performed testing on a sample of five movers to establish whether they had a completed and signed the user amendment form and had been set up with the correct privileges as per their job roles.<br><br>We further performed testing on a sample of five leavers and confirmed | Low | 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. | Completed (June 2019) | Kevin Willans, IT Manager |

| Ref | Control | Adequate control design (yes/no) | Controls complied with (yes/no) | Audit findings and implications | Priority | Action for management | Implementation date | Responsible owner |
|---|---|---|---|---|---|---|---|---|
| | | | | that all users accounts had been disabled.<br><br>Whilst audit testing did not note any issues with the creation and amendment of users account privileges and the disabling of users accounts; we were not able to obtain an audit trail by the way of a completed form for movers and leavers. Therefore, there is a risk that TfN is unable to provide assurances that the information about movers and leavers has been effectively communicated and acted upon.<br><br>In addition, discussion with management confirmed that TfN does not have a formally documented movers and leavers process. This increases the risk that procedures are not being completed in a consistent manner, which may lead to a user account being created with inappropriate permissions, or an account not being disabled in a timely manner. | | | | |

# APPENDIX A: 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 risks:

| Objective of the risk under review | Risks relevant to the scope of the review | Risk source |
|---|---|---|
| To provide assurance over TfN's control framework for managing cyber security risks to ensure TfN's resilience to security threats. | Loss of information, risks from inappropriate and malicious access, viruses and malware leading to data leakage, financial loss and/or litigation. | Internal Audit Plan |

---

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

An assessment of the high-level controls focussing on:

**Information Risk Management**

- Completion of any risk assessments or business impact assessments.
- Senior managements oversight and responsibility towards Information Risk Management.

**Secure Configuration**

- 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**

- Firewall rules and settings.
- Intrusion detection and prevention.

**Home and Mobile Working**

- Inspection of remote working approvals for employees working remotely.
- The relevant policies and procedures in regard to home and mobile working.

- The methods and security measures in place for staff who connect remotely into UKG's network.

**User Education and Awareness**

- User education and awareness in respect of cyber risk.

**Incident Management**

- Detection of security breaches or unauthorised access attempts.
- Incident management and reporting process, including lessons learned.

**Managing User Privileges**

- Process for user account creation, deletion and amendment.
- 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.

**Limitations to the scope of the audit assignment:**

- The scope of our work was 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.

- The information provided in our report should not be considered to detail all errors or risks that may currently or in the future exist within the IT environment, and it will be necessary for management to consider the results and make their own judgement on the risks affecting the organisation and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised.

- Any testing undertaken as part of this audit was on a sample basis for the current financial year only.

- We did not perform penetration testing or vulnerability assessments. The review was limited to identifying the existence of controls in the areas for review and obtaining supporting documentation.

- The data backup processes is not covered in this review. Testing was not undertaken to confirm that backups have been successful.

- IT Disaster Recovery was not included within this review. Information security/ data protection perspective will not be included within the review.
- Our work does not provide any guarantee against errors, loss or fraud or provide assurance that error, loss or fraud does not exist.

# FOR FURTHER INFORMATION CONTACT

**Lisa Randall, Head of Internal Audit**
07730 300 309
lisa.randall@rsmuk.com

**Sarah Massel, Assistant Manager**
07484 040 612
sarah.massel@rsmuk.com

**John Bradshaw, Technology Risk Manager**

07800 617054

john.bradshaw@rsmuk.com

**rsmuk.com**