TRANSPORT FOR THE NORTH

IT Access Management Security

Internal audit report 3.23/24

Final

16 January 2024

This report is solely for the use of the persons to whom it is addressed.
To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party.

1. EXECUTIVE SUMMARY

Why we completed this audit

Following two previous Cyber Security audits in 2020/21 and 2021/22, alongside a General Data Protection Regulation audit in 2022/23, we have conducted an IT Access Management Security review as part of the 2023/24 internal audit plan. This included the risk associated with control over staff and third party access to organisational systems and data held accessed through SharePoint sites and the Virtual Private Network (VPN).

Transport for the North (TfN) serves as a partnership bringing together transportation authorities and business leaders from the North with national transportation entities such as Network Rail, National Highways, and Central Government. Therefore, there is a heavy reliance on bi-lateral sharing of information and regular employment of external contractors in day-to-day operations. This audit focused on controls over the provisioning, monitoring and removal of access to TfN's systems and data, and how access security controls are applied in practice to staff and third parties.

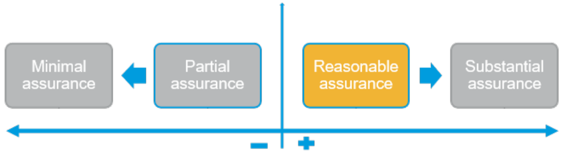
Conclusion

We identified that TfN has key controls in place to manage staff and third party access to TfN data and systems. However, some control weaknesses exist and require prompt management attention, particularly concerning the evaluation of third parties prior to granting them access to organisational data and the lack of ongoing verification to verify the suitability of staff and third party access. We also identified an issue with the management of privileged accounts, which was rectified during the audit. This was given immediate focus and attention by management to address this during our fieldwork, recognising this as a potential risk to the organisation and therefore this has been considered when determining our overall opinion. Action is also required to improve control over access provision and revocation, particularly with regard to contractors. Moreover, there is a lack of formalised and documented policies and procedures on access management for staff and third parties, despite a process existing in practice.

Internal audit opinion:

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



Key findings

We identified the following findings, resulting in four medium priority management actions being agreed. We also agreed four low priority management action which is detailed in section 2 below.

Third party Assessments

We were informed that no third parties had been onboarded over the last year and were unable to obtain evidence of the third party onboarding procedure being followed in practice. The onboarding process is defined within the IT Security Policy and IT Policy, however there is a lack of clarity on roles and responsibilities regarding this procedure. Privacy Impact Assessments have been conducted by the Legal team in the past but, third parties' security arrangements and associated risks are not assessed prior to granting them access to organisational systems and data. There is an increased risk of data breaches and third parties becoming sources of cyber-attacks. **(Medium, MA1)**

User Access Reviews

User access reviews are conducted primarily on a licensing basis. Whilst monitoring of licences is generally good practice to ensure that the organisation is not overpaying for unused or unnecessary licences, user access reviews against current employees should be conducted on a regular basis to ensure that all user access is appropriate and commensurate with job roles. Further, verification of third parties with access to SharePoint sites should be conducted periodically by SharePoint site owners. Not doing so increases the risk of unauthorised access to organisational data. **(Medium, MA2)**

Identity and Access Management – Policies and Procedures

Whilst there is a process in place for granting, amending, and revoking access to organisational systems, there is no policy in place to document this procedure. Further, it is stated within the IT Security Policy that staff will be required to undertake appropriate training before being granted access to organisational systems; however, which training is required for specific systems has not been defined. Additionally, we noted there is no formalised and documented process for granting third parties with access to SharePoint sites; access is granted on an ad hoc basis by designated internal owners of SharePoint sites. This may lead to user errors, inconsistent procedures, and unauthorised access to organisational data. Consequently, there is an increased risk of compromise to data integrity or data confidentiality. **(Medium, MA3)**

Identity and Access Management – Contractor Accounts

Accounts for contractors are not technically enforced to expire in line with leaving dates, which are recorded on new starter forms when the contractor starts work. This may result in unauthorised access to organisational systems and data, potentially leading to data breaches, insider threats, or misuse of privileges. **(Medium, MA4)**

Privileged Account Management

Within Azure Active Directory (AAD), we noted a global administrator account which was not separated from the user’s standard account. Having administrator accounts separated from standard user accounts reduces the risk of unintentional actions, narrows the attack surface on administrator accounts, and isolates administrative privileges to reduce the potential impact on the organisation in the event of a regular user account becoming compromised. This issue was corrected during our fieldwork and we have therefore not included a management action.

We noted the following controls to be adequately designed and operating effectively:

✓ Multi-Factor Authentication (MFA) is enabled for all members of staff, including those accessing organisational data via the VPN.

✓ There is a regular review of the validity, usage, and allocation of Microsoft 365 E3 licences held by the organisation.

✓ The organisation’s risk management approach has been clearly documented, and a dynamic tool is used to record, review, update, and manage risks across the organisation.

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: Third party Assessments		
Control	The IT Security Policy and IT Policy outline the procedure for third party assessments; this includes, but is not limited to: • A Data Assessment to determine security implications and control requirements, where there is a business need for working with external parties requiring access to TfN's information and information processing facilities. • A business case agreed between the requesting manager and the Information Technology Manager for third party suppliers with direct access to organisational IT systems. • Demonstration of compliance with ISO27001 and, where this requirement cannot be fulfilled, a risk assessment completed with approval from the Data Protection Officer (DPO) and risk acceptance from the Senior Information Risk Owner (SIRO). It is stated within the IT Security Policy that the IT and Information Department, led by the Information Technology Manager, are responsible for supporting the implementation of this Policy, including 'discussion' of the adequacy of third party supplier data security controls. Risk assessments are to be conducted when a third party cannot demonstrate ISO27001 compliance. Third parties are also required sign a Data Processing Agreement (DPA) when a supplier is processing personal data.	**Assessment:** **Design** ✓ **Compliance** ×
Findings / Implications	We noted that the IT Security Policy and IT Policy outline that risk assessments are to be conducted only when a third party cannot demonstrate ISO27001 compliance. Whilst ISO27001 is a widely-recognised international standard for Information Security Management Systems (ISMS), it may not cover all risks or requirements of TfN. Conducting risk assessments on all suppliers, including those with ISO27001 certification, ensures a more comprehensive understanding of potential risks facing the organisation in the context of third parties. We were informed that no new partners had been onboarded since the Information Technology Manager took on their role and were unable to obtain evidence demonstrating the third party onboarding procedure nor any third party risk assessments being followed in practice. However, we did confirm that Privacy Impact Assessments are conducted by the Legal team to assess the impact of sharing data and access to SharePoint and obtained examples of Data Processing Agreements that are in place with third party partners. Further, there is no centralised tracking of whether these required checks had been completed, as there is no third party register. Therefore, the organisation does not have effective oversight of whether the risks associated with third party access to organisational systems and data have been assessed. Third parties with inadequate security measures may become a source of data breaches or cyber-attacks, and there is a risk of GDPR non-compliance if the organisation has not assessed the security of data entrusted to third parties.	

Area: Third party Assessments				
	Additionally, there are no security policies and conditional access policies assigned to third parties when accessing SharePoint sites. Inadequate access control increases the likelihood of unauthorised users gaining access to SharePoint sites, potentially compromising the security of the sites and the integrity and confidentiality of the data they contain.			
Management Action 1	Management will: • Consolidate the procedure for third party assessments into a single policy, to ensure the process for onboarding and providing access to third parties is clearly outlined, alongside TfN roles and responsibilities in this process; • Amend this policy to ensure that risk assessments are conducted for all third parties, rather than just those lacking ISO27001 certification; • Ensure organisational policies and procedures on third party assessments are adhered to before granting access to organisational systems and data; • Create and regularly update a third party register to detail: ○ Notes on contract terms and the role of the third party; ○ The internal manager of this third party relationship (contract owner); ○ The level of access third parties have to organisational systems and data, including whether they process personal data; ○ Whether a DPA is in place; ○ A summary of the business case for third party access; ○ Whether the third party complies with ISO27001; and ○ Results of data assessments and risk assessments. • Investigate what conditional access policies can be applied to third party access to SharePoint, such as Multi-factor Authentication, and apply conditional	**Responsible Owner:** Danny Chapman, Information Technology Manager Gavin Legg, Governance, Data Protection and Contracts Lawyer	**Date:** 30 April 2024	**Priority:** Medium

Area: Third party Assessments	
	access policies where possible and where not, consider what additional access controls can be established.

Area: User Access Reviews

Control

User access reviews are conducted primarily on a licensing basis, rather than to ensure user access is appropriate and commensurate with job roles.

Assessment:	
Design	×
Compliance	N/A

Findings / Implications

Whilst monitoring of licences is generally good practice to ensure that the organisation is not overpaying for unused or unnecessary licences, user access reviews should be conducted on a regular basis to ensure that all user access is appropriate and commensurate with job roles. During our review, we noted the following issues relating to user access:

- 199 Azure Active Directory (AAD) ‘guest’ (external) accounts, some of which had last been modified as far back as 2017.
- 169 AAD ‘member’ (internal) accounts which could not be uniquely attributed to a current member of staff, as per the HR listing provided. These included:
  - Accounts created for shared or temporary purposes, i.e., ‘Facilities’, ‘Christmas’, and ‘Reserve a Manchester Office Deskspace’;
  - Accounts were merely attributed to devices, i.e., ‘Apple Device’ and ‘Apple ID’; and
  - Test accounts had been kept active and not disabled/deleted when not in use, for example, 'TfN Account', 'TestMfa', and 'test.contentgate'.
- We noted a number of accounts named as SharePoint site owners which we could not link to employees on the HR listing. Whilst management indicated that some are contractors, and therefore would not appear on the provided HR listing, five were individuals who had left the organisation who were designated as SharePoint site owners, and three of the five also remained enabled on AAD.
- There are no user access reviews conducted on SharePoint sites; instead, access is revoked when accounts have been inactive for a 60-day period. Whilst this will remove inactive accounts, it will not highlight third party partners that continue to access SharePoint even if their current role no longer requires this.

Without user access reviews, there is a risk that former employees, contractors, or external third parties retain access to organisational systems or data beyond that which is necessary or required for their role. Consequently, this increases the risk of unauthorised access to organisational data. Additionally, without reviewing and validating account existence and permissions, there is an increased likelihood that security incidents remain undetected.

Management Action 2		**Responsible Owner:**	**Date:**	**Priority:**
	Management will conduct user access reviews on a regular basis, by consulting with organisational units and SharePoint site owners to validate that user access aligns with job roles and responsibilities. Documentation of the review and any actions taken to adjust access will be maintained to enhance accountability and for audit purposes.	Danny Chapman, Information Technology Manager	29 March 2024	Medium

Area: Identity and Access Management – Policies and Procedures				
Control	Whilst there is a process in place for granting, amending, and revoking access to organisational systems, there is no documented policy in place to detail this procedure. Further, it is stated within the IT Security Policy that staff will be required to undertake appropriate training before being granted access to organisational systems. However, which training is required for specific systems has not been defined.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	Without clear policies in place, there is a risk that these procedures are not consistently followed, leading to employee frustration from delayed access to systems and resources, inappropriate user access permissions for their roles, or access not being revoked in a timely manner. Additionally, the absence of guidance on which training should be provided prior to granting users with access to certain organisational systems and data may result in staff not receiving suitable training. This may lead to user errors, inconsistent procedures, and reduced productivity resulting from users' unfamiliarity with system navigation and functionality. Consequently, there is an increased risk of compromise to data integrity or data confidentiality. Additionally, we noted there is no formalised process for granting third parties access to SharePoint sites. Whilst there are designated owners who are responsible for managing access to individual sites, the process for granting, amending, and revoking third party access to these SharePoint sites was unclear and not formally defined within a policy. Hence, there is an increased risk of inconsistent procedures, unauthorised access to organisational data, and compromise of data integrity or confidentiality.			
Management Action 3	Management will create a policy detailing the roles and responsibilities, and processes for: • Onboarding users (including training prerequisites), amending user access, and terminating user access; and • Granting, amending, and revoking third party access to SharePoint sites. This policy will be reviewed and approved by the highest level of delegated authority before being disseminated to the relevant stakeholders. Management should also ensure this defined procedure is followed in practice.	**Responsible Owner:** Danny Chapman, Information Technology Manager	**Date:** 31 March 2024	**Priority:** Medium

Area: Identity and Access Management – Contractor Accounts				
Control	Contractor leaving dates are recorded on the relevant new starter form, but accounts for contractors are not technically enforced to expire in line with these leave dates.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	If contractor leaving dates are not enforced, there is a risk that contractors retain access to organisational resources for a longer duration than required. This may result in unauthorised access to organisational systems and data, potentially leading to data breaches, insider threats, or misuse of privileges.			
Management Action 4	Management will: • Set contractors' access to expire in line with their contract end (leaving) date; • Ensure the contract owner and contractor are suitably notified when the account is approaching expiry; • Where access is required to be extended, this will be requested through a Service Desk ticket with suitable approval obtained; and • Ensure that the new Access Control Policy (as per Management Action 4) appropriately reflects this process.	**Responsible Owner:** Danny Chapman, Information Technology Manager	**Date:** 15 March 2024	**Priority:** Medium

Area: Incident Management				
Control	There is an Incident Management Procedure documented within the IT Security Policy, and incidents are recorded on the Service Desk. Incidents are reported into the IT Strategy Group and the Senior Information Risk Officer (SIRO) to identify any lessons learnt from the types, severity and prevalence of cyber-related incidents.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	We noted that the Help Desk and incident management process was tested as part of its onboarding, however, there was no clear testing strategy for the incident management process in the future. Penetration testing is conducted, however, unless this is carried out as a Red Teaming exercise (i.e. an exercise to emulate a real-world cyber attacker), this will not also test the incident management procedure. Without conducting regular security and incident response tests, there is a risk that the incident management processes may not be operating as expected; testing helps identify gaps or missing elements within the plan, such as incomplete contact lists, procedural errors, miscommunications, or resource shortages. Identifying and addressing any errors in a controlled test environment helps to prevent them in the event of an actual cyber security incident.			
Management Action 5	Management will develop a strategy for periodic testing of the incident management procedure to validate its effectiveness, ensuring that there is a lessons learnt exercise following these tests to continually improve the plan.	**Responsible Owner:** Danny Chapman, Information Technology Manager	**Date:** 29 March 2024	**Priority:** Low

Area: Risk Management				
Control	The organisation has a risk register which is regularly reviewed and updated to reflect the risks facing the organisation.		**Assessment:** **Design** **Compliance**	 ✓ ×
Findings / Implications	The risk rating for 'Data Access Reviews', described as "risk of breach of data access compliance with new and legacy users accessing data from TfN's Sharepoint/Azure Systems", should be re-assessed in light of the findings highlighted by this audit. We have noted several findings relating to access management within this audit, particularly in respect to the provisioning and removal of access to third party partners. Whilst the distributed authority to allow access to SharePoint sites forms a part of TfN’s operating model it does relinquish some control over who can access SharePoint sites and the 'low threat' rating associated with this risk item could be deemed lower than the actual risk accepted. Underestimating this risk may lead to inadequate allocation of resources to manage this risk effectively. Subsequently, this may lead to unanticipated outcomes if this risk becomes actualised.			
Management Action 6	Management will re-assess the risk rating associated with Data Access Reviews to ensure that it accurately reflects the current risk level, and ensure there are appropriate plans in place to mitigate this risk or formally accept a higher level of risk.	**Responsible Owner:** Danny Chapman, Information Technology Manager	**Date:** 29 February 2024	**Priority:** Low

Area: Identity and Access Management – Leavers				
Control	User accounts are disabled, not deleted, when no longer required.		**Assessment:**	
			Design	×
			Compliance	N/A
Findings / Implications	Upon inspection of the AAD user listing, we noted user accounts are disabled instead of deleted when users no longer require access. Therefore, the organisation has 1,200 disabled accounts within AAD. Disabled accounts could be exploited by malicious actors if they are not deleted, as they could be reactivated and used for fraudulent activity. There is an increased risk of unauthorised or inappropriate access to organisational systems and data leading to a breach of data integrity or confidentiality. It should be noted, however, there are business cases for keeping accounts disabled instead of deleting them, such as for staff members on temporary leave, or data retention (i.e., emails, documents audit logs) for legal or compliance purposes.			
Management Action 7	Management will: • Delete user accounts when no longer in use; • Where there is a business case for accounts to remain disabled (i.e., not deleted), ensure requests are raised through the Service Desk as part of the leaver request; and • Establish clear policies and procedures for managing disabled accounts in order to reduce security risks and ensure they are managed appropriately based on organisational requirements.	**Responsible Owner:** Danny Chapman, Information Technology Manager	**Date:** 29 February 2024	**Priority:** Low

<table>
<tr><th colspan="5">Area: Privileged Account Management</th></tr>
<tr><td><b>Control</b></td><td colspan="2">Global administrator accounts are used to manage SharePoint sites and have access to Virtual Machines via the Virtual Private Network (VPN).</td><td><b>Assessment:</b>
<b>Design</b>
<b>Compliance</b></td><td>
×
N/A</td></tr>
<tr><td><b>Findings / Implications</b></td><td colspan="4">We noted violations of the principle of least privilege in the context of global administrator account usage:
• Two instances where global administrator accounts were named owners of SharePoint sites.
• Two instances where global administrator accounts had Virtual Private Network (VPN) permissions in order to access Virtual Machines (VMs).
In both instances, the use of global administrator account permissions exceeds the privileges required for the specific tasks at hand. Therefore, this violates the key security principle of least privilege, which stipulates that only the minimum level of access required to perform tasks should be granted, in order to reduce the risk of security breaches and limit potential damage if a breach does occur. Hence, using these accounts for tasks where global administrator privileges are excessive increases the risk of unauthorised access to organisational data and potential misuse of elevated access rights, leading to data leaks, data loss, and operational disruption.</td></tr>
<tr><td><b>Management Action 8</b></td><td>Ensure all account permissions align with the principle of least privilege, having only the necessary access to perform their specific functions.</td><td><b>Responsible Owner:</b>
Danny Chapman, Information Technology Manager</td><td><b>Date:</b>
29 February 2024</td><td><b>Priority:</b>
Low</td></tr>
</table>

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
Cyber disruption/attacks to the available information and technical infrastructure. Inappropriate user access to confidential information. Access may be limited for an unknown period of time.	6	2	4	4	0
Total			**4**	**4**	**0**

APPENDIX B: 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 risks:

Objective of the review	Risks relevant to the scope of the review	Risk source
To provide assurance that the processes in place to manage user and third party access to systems and data are in line with good practice.	Cyber disruption/attacks to the available information and technical infrastructure. Inappropriate user access to confidential information. Access may be limited for an unknown period of time.	Risk Register

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

The audit will consider the following;

1. Risk Management

- The risk management process (identification, assessment, treatment, monitoring).
- The risk posed by third party access to data TfN is responsible for is understood, mitigating controls and risk treatment plans have been established.

2. Identity and access management

- Definition or policy of identity and access management for staff accounts and third party access to SharePoint.
- Authorisation model and procedures (e.g. account creation, deletion and amendment) for staff users and third party access to SharePoint.
- Authentication for end user accounts, including password policy and Multi-factor Authentication (MFA).
- Restrictions to privileged accounts (e.g. administrative accounts) and access to the VPN (staff and any third parties that have access).
- Monitoring of account usage and accesses (for both staff and third party access).
- Use of service accounts and the privileges assigned to service accounts.
- Reviews of staff access and reviews of third party access to SharePoint are undertaken.

3. Security over third party access

- Third parties are assessed ahead of being granted access to SharePoint sites.
- Third parties are required to sign an Acceptable Use Policy and/or a Data Processing Agreement before access to SharePoint sites is granted.
- Security policies and conditional access policies are assigned to third parties when accessing SharePoint sites.

4. Incident management

- Incident management and reporting process, as well as lessons learnt.
- Detection of security breaches or unauthorised access attempts.

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 IT/cyber security.
- The approach taken for this review will be to validate the design of key controls and will not include all monitoring controls.
- We will be testing only selected key controls and on a sample basis 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 IT environment, and it will be necessary for management to consider the results and make their own judgement on the risks and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised.
- The results of our work are reliant on the quality and completeness of the information provided to us.
- In addition, our work does not provide an absolute assurance that material error; loss or fraud does not exist.

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

Debrief held	8 and 27 November 2023
Final information received	14 and 29 November 2023
Draft report issued	21 November 2023 and 13 December
Revised draft report issued	13 December 2023
Responses received	15 January 2024
Final report issued	16 January 2024

Internal audit Contacts	Lisa Randall, Head of Internal Audit (IA) Alex Hire, Associate Director (IA) Ciaran Barker, Assistant Manager (IA) Anna O'Keeffe, Director, Technology Risk Assurance (TRA) Wil Milligan, Manager (TRA) Tom Wilkinson, Senior Consultant (TRA) Muhammed Patel, Consultant (TRA)
Client sponsor	Danny Chapman / Information Technology Manager
Distribution	Danny Chapman / Information Technology Manager

We are committed to delivering an excellent client experience every time we work with you. If you have any comments or suggestions on the quality of our service and would be happy to complete a short feedback questionnaire, please contact your RSM client manager or email admin.south.rm@rsmuk.com

.

rsmuk.com

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 UK 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 UK 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 UK 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.