TRANSPORT FOR THE NORTH

Review of SharePoint

Internal audit report: 4.19/20

FINAL

12 November 2019

EXECUTIVE SUMMARY

Why we completed this audit

An audit of Transport for the North's ('TfN')'s SharePoint system was undertaken as part of the approved internal audit plan. TfN utilise the Microsoft cloud-based collaborative product SharePoint Online as a means of publishing and sharing information internally and externally with key third parties.

The objective of the review was to assess the strength of the controls in place over the SharePoint system and its contents are protected from risks of misclassification, disruption, unauthorised access and data loss.

SharePoint is provided as part of the Office365 suite. Azure Information Protection is used to classify documents and emails within it. Management noted that whilst there is some sensitive data held in SharePoint, it is limited in nature.

The audit was carried out primarily through sample-based testing of controls, meetings with the Head of IT and Information along with a review of key documentation relevant to the scope.

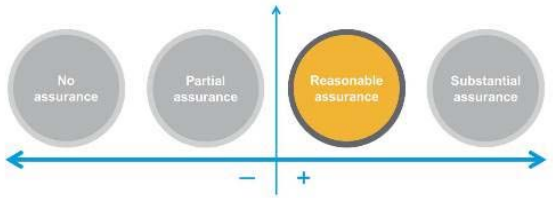
Conclusion

The audit has highlighted that some control improvements are required with a view to enhancing and strengthening the control framework. Two medium priority management actions and three low priority management actions have been raised for consideration by Management. A formal assurance opinion has been provided below.

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 the identified area are suitably designed, consistently applied and operating effectively.

Appendix B shows the different opinions and their definitions.



Key findings

All staff have the ability to create sites which can be shared with third parties (TfN had 89 external share sites at the time of the review). This poses the risk that site owners may establish sites with incorrect security settings and that they may not be able to monitor storage of sensitive data that could lead to inappropriate access or data loss of personal or business sensitive data. Without oversight and control of external sites, there is a risk that TfN may lose sight of where organisational data is stored and exposed as there will be no indication of how external sites are being used or what data third-parties have access to them.

TfN does not have an established sharing whitelist to formally control external sharing with third party users. Industry best practice suggests identifying partner companies and creating a list of domains, with whom content is to be shared and hence managing a sharing whitelist. A sharing whitelist limits the access of unknown entities and protects the network's resources. There is a risk that TfN does not have sufficient controls in place over external data sharing which can in turn pose a significant threat for the organisation through unauthorised data access or leakage.

Other than the default retention rules (seven years and seven months), TfN has not established formal retention and deletion rules to manage third party and internal user access to Site Collections when it is no longer required. Without effective records management through the timely retention and deletion of records; there is a risk of unauthorised access to Site Collections by third parties or internal users which no longer require access to such data. This increases the risk of the potential leakage of sensitive information.

Observations

In discussion with the Head of IT and Information, we were informed that there have been instances where multiple sites have been created for the same purposes, usually by different functions within TfN who are working on the same document. For example, the Business Support Team and Legal Team both maintained a governance agenda that caused duplication when communicating to stakeholders. This increases the potential risk of duplicating personal sensitive information that compromises data protection principles on accuracy and accountability. However, following this specific occurrence, the Head of IT and Information performed additional training and aligned governance folders to allow for greater joint working. In addition, TfN's planned movement to Metadata in order to restructure its core services, allows for a movement away from siloed folder structures, which should therefore remove these issues in the future.

In discussion with the Head of IT and Information we were informed that TfN has provisioned Bluesource to categorise and archive repositories, and hence create new Metadata depositaries within SharePoint. We obtained evidence confirming that TfN has defined a structure for the Metadata. However, it is currently under review with Bluesource. Upon formal approval, we were advised by the Head of IT and Information that Bluesource indicated a 12-week deployment process.

The outsourcing of this work is intended to help establish categories and naming standards to introduce consistency across a SharePoint deployment and support comprehensive enterprise Metadata management. This provides a detailed roadmap from which TfN content users and information workers can easily discover and locate the information they need to solve business problems. The aim of TfN is to initially focus on Programmes and Projects but are aiming to also move across the core business once it is established.

Controls operating effectively

Whilst we acknowledge much of TfN's data will be made publicly available in line with the principle of data openness. We confirmed that a data classification scheme (Public; Internal; Restricted; and Confidential) has been implemented and that protective marking is enforced at document creation by the Microsoft Office suite. This was confirmed through TfN's ability to monitor all sensitive data within SharePoint through using a 'sensitive' tag to retrieve all data which has been marked with this level of classification within the Sites. Classification and identification of sensitive data is critical to proper governance. By understanding where sensitive data lies, SharePoint administrators can then lock down relevant sites through access management and appropriate permission structures. This allows TfN to have ease in enforcement of risk management, compliance and data security. This is in turn allows TfN to more effectively adhere to compliance regulations.

We obtained audit logs confirming that the Head of IT and Information conducts quarterly recertification checks of SharePoint sites. Monitoring what actions are being taken and who has control of Site Collections is critical when meeting regulatory compliance and records management. Through conducting regular audits, TfN can filter and locate any unauthorised or suspicious activity, and hence better control data governance. All suspicious activity is followed up by the Head of IT and Information to ensure effective and timely resolution.

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.

Risk or Area: Security Control Environment				
Control	All staff have the ability to create sites which can be shared with third parties. TfN has 89 sites which are externally shared.		**Assessment**	
			Design	×
			Compliance	n/a
Findings / Implications	There is limited governance and control over the creation of sites that allow external access to data. In discussion with the Head of IT and Information we were informed that all staff are able to create sites allowing external data sharing with third parties. We confirmed that quarterly audit checks are performed by the Head of IT and Information to verify that third party users and their granted permissions continue to remain appropriate. At the time of our review we noted that in excess of 89 sites had external sharing enabled. This increases the risk exposure by having too many external access points to data that are reliant upon the quarterly monitoring. There should be an additional level of security approval and justification in place before a user is able to grant an external party access to a SharePoint site, especially for sites which contain sensitive data. Without such governance and control of external sites, there is an increased risk that TfN may lose sight of where organisational data is exposed as there will be no indication of how external sites are being used or what data third-parties have access to.			
Management Action 1	Management will review their processes for creating external shares. This should include an assessment of the sites purpose, the sensitivity of data and those who will have access to the data. Furthermore, management will assess the requirement for having an additional level of security approval from the Heads of Department before granting an external party access to a site.	**Management Comment:** Investigation into the options available to pursue this action will take place. There is currently no “in tool” solution to provide this requirement. **Responsible Owner:** Head of IT and Information	**Date:** 30 November 2019	**Priority:** Medium

Risk or Area: Security Control Environment		Assessment	
Control	TfN has not implemented appropriate controls in order to ensure that access to data is revoked once it is no longer required.	**Design**	×
		Compliance	n/a
Findings / Implications	Through review of TfN's default retention policy we confirmed that TfN has applied a retention policy of seven years and seven months for systems within the organisation such as Office 365 and SharePoint. In addition to the default retention policy, data is also deleted via site audits by the Head of IT and Information, which are carried out on a quarterly basis, or when requested by the site owners. However, we confirmed that other than the quarterly audit checks which rely heavily upon the site owners understanding of data governance, TfN not implemented any additional technical controls to monitor user activity within the site and subsequently remove it if it is no longer required. We were informed by the Head of IT and Information that often additional sites are created and used by internal users, i.e. for different stages of projects. These are not normally deleted after use as they may be referred back to in the future. Hence, the default retention policy can be appropriate for internal users. However, the need for third parties to be able to access data for seven years and seven months is significantly reduced and should be addressed by TfN. It is good practice to have effective records management through the timely retention and deletion of records, as per the data protection policy. There is a risk of unauthorised access to Site Collections by third parties or internal users which no longer require such data.		
Management Action 2	In addition to the current default retention policies in place, management will look to add specific site policies, particularly for those sites used by third parties, such as through a retention rule of 60 or 90 days for third-party sites.	**Management Comment:** Agreed with finding and will instigate a Retention Policy for 3rd party associated SharePoint sites. **Responsible Owner:** Head of IT and Information	**Date:** 31 October 2019	**Priority:** Medium

Risk or Area: Security Control Environment				
Control	Missing control: TfN has established a whitelist of partner companies through which they share content with.		**Assessment** **Design** **Compliance**	 × n/a
Findings / Implications	We obtained verbal confirmation from the Head of IT and Information that TfN does not have an established sharing whitelist to formally control external sharing with third party users. Industry good practice suggests identifying partner companies and creating a list of domains, with whom content is to be shared and hence managing a sharing whitelist. This protects the network's resources and limits the access of unknown entities. Whilst we acknowledge that TfN has advised staff to not create external shares with partners and third parties who use generic email accounts such as Gmail, Hotmail, Yahoo, etc., technical controls have not been enforced to manage this process. Although the list of external users is manually monitored by SharePoint administrators, this is monitored on an ad-hoc basis only. There is a risk that TfN does not have sufficient controls in place over external data sharing, which can pose a significant threat for the organisation through unauthorised data access or leakage.			
Management Action 3	Management will consider the implementation of a whitelist and blacklist domains for external sharing. Following this, these lists should be regularly updated depending on change in domain partners, through removal of permissions and accounts.	**Management Comment:** Management action agreed and we will work with the Legal team to generate, communicate and maintain an approved whitelist of Partners and Suppliers. **Responsible Owner:** Head of IT and Information	**Date:** 30 November 2019	**Priority:** Low

Risk or Area: System Resilience				
Control	TfN adopt the native Microsoft SharePoint Online backup arrangements. Microsoft will make a backup every 12 hours and keep it for 14 days. After this period Microsoft is unable to restore customers site collections.		**Assessment**	
			Design	×
			Compliance	n/a
Findings / Implications	We were informed by the Head of IT and Information that TfN rely on the backup arrangements of Microsoft for the backup of SharePoint. We were further advised by the Head of IT and Information that TfN investigated the costs of having a third party manage their SharePoint Online backup. This would offer flexible retention options (retain weeks/months/years of incremental data to restore from) as well as a granular restore process, enabling TfN to restore individual file or list items as well as the restoration of an entire site collection of a library as they found the costs to be prohibitive and had therefore accepted the risk of continuing without. However, the Head of IT and Information could not confirm if the acceptance of this risk probability and impact had formally been recorded in line with TfN's risk appetite. A lack of documented risks surrounding the backup controls exposes TfN to the risk that the current decision is not periodically challenged, to confirm that as the organisation evolves, control should not be enhanced.			
Management Action 4	Management will consider formally recording the acceptance of the risk of not having a third party to manage the backup of SharePoint Online as part of the risk register.	**Management Comment:** Risk acceptance documentation completed and awaiting formal sign-off. **Responsible Owner:** Head of IT and Information	**Date:** 30 November 2019	**Priority:** Low

Risk or Area: Third Party Management				
Control	Missing control: Data sharing agreements are in place with all third parties with whom TfN share business and personal data.		**Assessment** **Design** **Compliance**	 × n/a
Findings / Implications	Other than the data processing agreement in place with Transport for Greater Manchester (TFGM), we were unable to obtain further evidences to confirm that data sharing agreements are in place with the third parties which we identified have been provided external access to data via SharePoint external sites. We sampled the TFGM agreement and found that this agreement had not been approved and was labelled 'v02 draft'. It is good practice to have a data sharing agreement in place with a third party. It sets out the purpose of processing and the obligations of the third party in safeguarding TfN's business and personal data. This will further benefit TfN by demonstrating their accountability for good data management which meets legal and regulatory requirements such as the GDPR and minimises the risk of data loss. There is a risk that staff may share data with third parties for whom TfN does not have an approved data sharing agreement in place.			
Management Action 5	Management will apply controls to ensure that the creation of external sites is limited to third parties for which TfN has an approved data sharing agreement in place.	**Management Comment:** Data Sharing agreement process, revised SharePoint site creation training and whitelist management will enforce improved TfN external data sharing. **Responsible Owner:** Head of IT and Information	**Date:** 31 December 2019	**Priority:** Low

APPENDIX A: CATEGORISATION OF FINDINGS

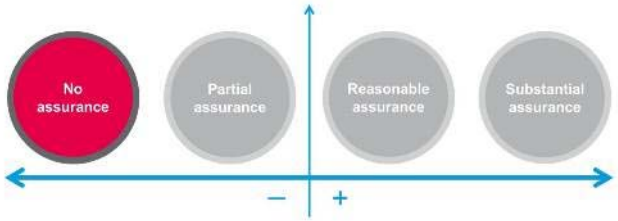
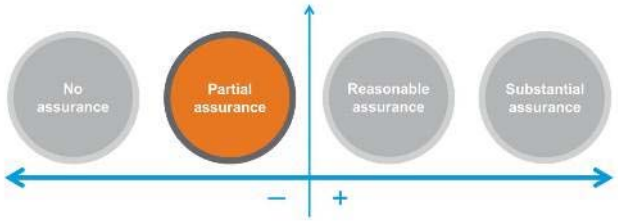
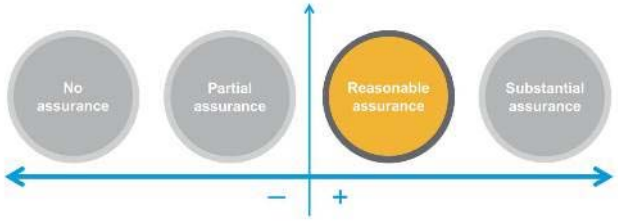
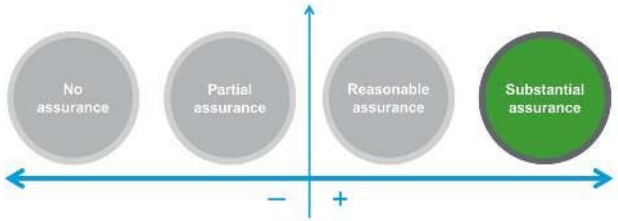
Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the 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
Data loss or unauthorised access lead to business disruption, data leakage and consequent financial and reputational damage	6	(27)	0	(27)	3	2	0
Total					**3**	**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: INTERNAL AUDIT OPINIONS

Graphic	Opinion
	Taking account of the issues identified, the Board cannot take assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective. Urgent action is needed to strengthen the control framework to manage the identified risk(s).
	Taking account of the issues identified, the Board can take partial assurance that the controls to manage this risk are suitably designed and consistently applied. Action is needed to strengthen the control framework to manage the identified risk(s).
	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(s).
	Taking account of the issues identified, the Board can take substantial assurance that the controls upon which the organisation relies to manage the identified risk(s) are suitably designed, consistently applied and operating effectively.

APPENDIX C: SCOPE

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 review	Risks relevant to the scope of the review	Risk source
The SharePoint system and its contents are protected from risks of misclassification, disruption, unauthorised access and data loss.	Data loss or unauthorised access lead to business disruption, data leakage and consequent financial and reputational damage.	Client meeting on 30 August 2019.

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

The audit will include a high-level consideration of the following areas relating to SharePoint and its use:

End user governance and policy

- The user administration process in place for new starters and leavers; and
- Access controls in place (including those governed by data classification).

Security Control Environment

- The existence and completeness of operating policies and procedures;
- The appropriateness of any administrator and privileged access;
- How permissions are granted and the extent of permissions allowed for internal users and external groups;
- Procedures in place over SharePoint guest accounts; and
- Remote access settings by staff and third parties.

System Resilience

- The completeness of existing IT disaster recovery arrangements for SharePoint;
- Procedures to be invoked should access to SharePoint be lost; and

- Back-up arrangements in place (as operated by Microsoft).

Data

- The process for correctly classifying and securing data stored in SharePoint;
- The adequacy of procedures for securing sensitive data (employee, suppliers, third parties); and
- Compliance with current GDPR requirements in respect of SharePoint.

Third Party Management

- The use of data sharing agreements with key third parties;
- Controls over sharing data from SharePoint with third parties; and
- Access rights to SharePoint by any third parties to access data.

User Training

- User training on appropriate use of SharePoint; and
- Staff training to those who create and modify user groups and permissions.

Monitoring

- Procedures to identify, manage and report incidents in relation to the use of SharePoint;
- The use of SharePoint audit tools and reports;
- Monitoring arrangements in place over the use and operation of SharePoint (including user take-up); and
- Service Operator Controls (SOC) arrangements in place with Microsoft.

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 upon in the areas for consideration in the context of the objectives set out for this review, and is not to be considered as a comprehensive review of all aspects of network management / security;
- This review will not cover how related third parties secure data that is shared with them by TfN;
- Conclusions will be based on our assessments made through discussions with management, assessment of the current framework of controls and an initial review of relevant documentation available, either internally or externally generated;
- Our audit will not seek to replicate advice provided to you by any third parties and external advisors; and
- The information to be provided in the final report should not be considered to detail all errors or risks that may currently or in the future exist within SharePoint 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.

Debrief held	25 September 2019, 21 October 2019 and 8 November 2019	**Internal audit Contacts**	Lisa.Randall@rsmuk.com / 07730 300309 Alex.Hire@rsmuk.com / 07970 641757 David.Morris@rsmuk.com / 07800 617128 Dom.Hamilton@rsmuk.com / 07436 268364 Munibah.Ahmed@rsmuk.com / 0161 830 4000
Draft report issued	21 October 2019 and 11 November 2019		
Responses received	11 and 12 November 2019		
Final report issued	12 November 2019	**Client sponsor**	Iain Craven – Finance Director Kevin Willans – IT and Information Manager
		Distribution	Iain Craven – Finance Director Kevin Willans – IT and Information Manager

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.