THE POLICE, FIRE AND CRIME COMMISSIONER FOR NORTH YORKSHIRE AND THE CHIEF CONSTABLE FOR NORTH YORKSHIRE

SharePoint Security

FINAL

Internal audit report: 14.18/19

7 May 2019

RSM

CONTENTS

Debrief held	10 January 2019	**Internal audit team**	Daniel Harris, Head of Internal Audit
Draft report issued	4 February 2019		Angela Ward, Senior Manager
Responses received	7 May 2019		Philip Church, Client Manager
			David Wayman, Principal Consultant
Final report issued	7 May 2019	**Client sponsor**	Interim Managing Director – Post 1st April
		Distribution	Interim Managing Director – Post 1st April
			Head of ICT

1 EXECUTIVE SUMMARY

1.1 Background

An audit of SharePoint Security was undertaken as part of the approved internal audit periodic plan for 2018 / 2019.

The force has for several years utilised the Microsoft web-based collaborative product, SharePoint, as a means of publishing and sharing information internally. A current project, nearing completion, upgraded the product to its 2016 version and the force took the opportunity to review security and permissions, following significant (but internal) data leaks from previous SharePoint sites.

SharePoint is the basis of the force's intranet, 'The Source' (actually around 160 sub-sites) and also a large number of team sites. Management's approach to access to data within these sites is that 'The Source' is open to all staff whereas access to team sites is determined by delegated site owners. Site owners take formal responsibility for monitoring and reporting upon the security of their sites whilst Information Asset Owners (IAOs) are also formally nominated for each sub-site and have formal responsibilities as summarised in the "Information Security Policy".

In the future the force may move to a 'cloud-based' implementation of SharePoint; issues raised in this report should therefore also be considered in the light of this potential development.

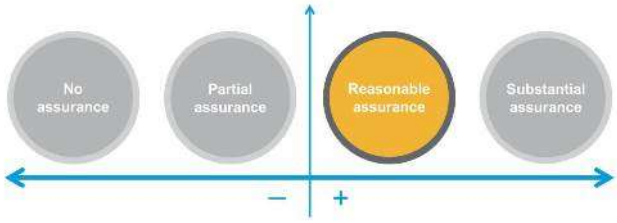
1.2 Conclusion

Whilst the approach taken to ensuring the security of the SharePoint implementation and of individual sites is a sound one, we have identified actions for improvement which have impacted our opinion.

Internal audit opinion:

Taking account of the issues identified, the Police, Fire and Crime Commissioner for North Yorkshire and the Chief Constable of North Yorkshire can take **reasonable assurance** that the controls in place to manage this area 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 area.



1.3 Key findings

The key findings from this review are as follows:

- We confirmed that management has demonstrated governance of the SharePoint upgrade and security implementation through areas such as security policies, delegation of site ownership and security administration, and training and guidance.
- We confirmed that management has implemented a set of information security policies to provide guidance to users on the appropriate and secure use of all information resources; these policies are available from 'The Source'. We also confirmed that specific guidance on the use of SharePoint has been made available, targeted to different levels of user.
- We confirmed that the SharePoint implementation is exclusively internal to the organisation. We confirmed that the North Yorkshire Police website is managed externally and that there are no links from the website to the Intranet or team sites. Remote or third-party access to the SharePoint sites is not permitted, thus reducing the risk of unauthorised access.

- We confirmed that a data classification scheme has been implemented and that protective marking is enforced at document creation by the MS Office suite, which we confirmed during the audit.
- We confirmed that access to SharePoint sites are restricted to authorised users through the use of authentication controls within Active Directory.
- We confirmed that a process of regular security auditing and reporting to management on the security and utilisation of sites has been established.
- We confirmed that a procedural requirement has been implemented that new sites can only be set up centrally, following a formal request and approval process. With improved technical controls (see detailed finding two) this control will help to prevent the sprawl of SharePoint sites and consequent loss of control over security.

We have agreed **one high** and **two medium** priority management actions in relation to the following:

- Reviewing selected access permissions from the generated permissions matrix, we noted a number of anomalies, such as:
  - Several users with both full control and full control NYP at site level. The latter permission was designed to allow full control minus the ability to create new sites, so the allocation of both permissions cancels the effectiveness of this approach;
  - 101 sites were found to have groups or users allocated with full control (a permission level discouraged at NYP for the reason outlined above); and
  - With respect to the HR site (which may be considered "sensitive") two users had been granted full control and two had been granted full control NYP. The group "HR Owners" had both full control and full control NYP. **(High)**
- Although training materials were developed as part of the current SharePoint upgrade project, management has acknowledged that there is little in the way of provision for ongoing training of site owners. Furthermore, there is no monitoring process in place to ensure that training is delivered effectively and that all those that require training actually complete the required modules. Failure to provide appropriate training for those with security responsibilities may result in security standards not being properly managed. **(Medium)**
- Management were not able to provide design documentation for the security of the SharePoint implementation. Whilst management decisions were taken at the time of the upgrade (such as not importing permissions from the legacy version but allocating these from the 'ground up') the absence of any design documentation may indicate a lack of planning for effective security, and a deficiency in the information governance process. The absence of security standards may also hinder effective auditing by site owners. **(Medium)**

We have agreed **three low priority management actions** and further details can be found in section two of this report.

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.

Area	Control design not effective*		Non compliance with controls*		Agreed actions		
					Low	Medium	High
SharePoint Security	2	(6)	4	(6)	3	2	1
Total					**3**	**2**	**1**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

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 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.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
1	Guidance on the use and administration of SharePoint has been created and published on the intranet in the form of user guides.	Yes	No	We noted that the training materials are either written guides or short videos. They are divided into those aimed at: • All intranet users; • Site owners; and • Administrators. The implementation of these training guides was part of the implementation project for SharePoint 2016, which is drawing to a conclusion. It has, however, been acknowledged by management that ongoing training may be lacking, and there is no QA review of training effectiveness. This in turn could lead to poor practice in the administration and security of SharePoint sites. **Risk Exposure** | **Root causes**	Medium	Management will ensure that a training programme for all site owners and identified IAOs is established to provide appropriate training in information security responsibilities relating to SharePoint. Attendance and completion of these courses should be monitored by management.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
				Risk that best practice principles for SharePoint security are not consistently applied, leading to data leakage. | Inadequate training programmes.		**Responsible Officer:** Data Protection Officer
				Probability | **Financial** | **Reputational** | **Operational** | **Legal** | **Rating** Probable | Minor | Probable | Minor | Probable | 5.8		**Implementation Date:** 31 December 2019
2	**Missing control** We noted in discussion with management an absence of security design documents for the SharePoint implementation.	No	-	We understand that the original ITT (for the original SharePoint implementation, prior to the current version) required the external provider to provide a security design to be applied (we confirmed that the high-level Intranet Project Plan includes the requirement to supply 'Information architecture, metadata, cross-site content types, security and permissions model') but there is no evidence that such a design exists within project folders. Although we have been advised that permissions were not transferred from legacy to 2016 SharePoint, we understand that information security requirements were not documented as part of the current project. Failure to document system security requirements may indicate deficiencies in the overall governance process, and can lead to inappropriate security settings and privileges being set through lack of organisational guidance. The absence of security standards for an application may also hamper the audit process (as performed by site owners) through an inability to benchmark actual security against standards.	Medium	Management will establish formal security standards for SharePoint, to provide a best practice benchmark to site owners, both for administration purposes and to assist with annual auditing and ongoing security monitoring. The standards should be consistent with the NYP Information Security Policy and take into account Microsoft SharePoint security best practice. **Responsible Officer:** DISG Apps and Data **Implementation Date:**
				Risk Exposure | **Root causes** Risk that best practice standards are not implemented at system implementation stage. | No formal security design documentation produced by the project.		

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
				Probability | **Financial** | **Reputational** | **Operational** | **Legal** | **Rating** Probable | Negligible | Probable | Minor | Probable | 5.8		30 September 2019
3	As part of the security implementation, the permission level full control has been modified as full control NYP, which prevents the creation of new sites.	Yes	No	We tested how many users or groups have full control against SharePoint objects and (restricting our outputs to sites and site collections) found that sites with full control assigned numbered 101 and site collections five. Given that full control is intended to be severely restricted, this number is very high. We also found 192 sites with full control NYP assigned to users or groups, and one site collection, 'The Source", with full control NYP (19 users or groups). Looking at one specific team site (HR) we noted that two users had been granted full control and two users had been granted full control NYP. We also noted that the group "HR Owners" had both full control and full control NYP. Additionally, we found two other sites (Information Management and Niche User Guides) where some users had both full control and full control NYP. Failure to restrict the ability to create new sites could lead to site proliferation in defiance of NYP policy and consequent breakdown in control of security standards, and may indicate overall deficiencies in the governance and communication processes. **Risk Exposure** | **Root causes** Risk that SharePoint sites are created without approval and that security standards deteriorate. | Failure adequately to restrict full control. **Probability** | **Financial** | **Reputational** | **Operational** | **Legal** | **Rating** Probable | Negligible | Negligible | Minor | Negligible | 5.8	High	Management will perform a full (and periodic) review of the permissions matrix to identify anomalies (including those identified during this audit), and investigation and remediation as required. **Responsible Officer:** DISG Apps and Data **Implementation Date:** 30 June 2019

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
4	An annual review of all sites is proposed to establish that they are still being used and are still required.	Yes	No	On the proliferation of sites, management advised that the number of sites (363, including some test sites) although large, is a significant reduction since the 2016 upgrade. The force data protection officer stated that the proposed annual review of sites will ask: • Is the site being accessed? • Is the number of sites comparable to similar organisations or forces? The details of this review (frequency, method, recording, follow-up, etc.) have not yet been documented. Failure to formalise the annual review of SharePoint sites could diminish its effectiveness and lead to site sprawl and reduction in security standards. In the absence of a formal taxonomy, management may find it difficult to assess the nature and purpose of sites. SharePoint taxonomy provides an optional, formal classification scheme for the systematic identification and arrangement of business activities and/or records according to logically structured conventions, methods and procedural rules, which are represented in categories or grouping of terms. The scheme is used to identify terms by which documents are grouped together to facilitate retrieval, compliance, storage and life-cycle management (including disposition). Developing a master classification or taxonomy schema for content filing would allow the organisation to apply consistent vocabulary control. Without a clear definition, poor or no taxonomy, there is a risk of unplanned and undesirable outcomes such as inconsistent naming standards, vague field names and a disorganised site structure making enterprise search capabilities difficult.	Low	Management will ensure that the auditing of site proliferation is formally documented as an audit procedure. Management may also wish to consider the formal design of a SharePoint taxonomy. **Responsible Officer:** Data Protection Officer **Implementation Date:** 30 June 2019

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
				Risk Exposure / **Root causes** Risk that sites proliferate and security standards diminish, leading to potential data leakage. / Annual audit of sites not adequately documented. **Probability** | **Financial** | **Reputational** | **Operational** | **Legal** | **Rating** Probable | Negligible | Probable | Minor | Negligible | 5:8		
5	Security breaches from SharePoint sites have been documented within the IT Risk Register.	Yes	No	We noted that the mitigating action documented in the IT Risk Register was very high level and long-term (implement an ISMS) and there was no tactical response (such as reviewing SharePoint permissions, auditing, training, etc). Management have advised that specific technical remedial action was taken to remedy these breaches but that the risk record was not updated. We also noted that these incidents do not appear to have been recorded within the incident management system, Sostenuto. Failure adequately to record actions taken to remediate security incidents could lead to a repetition of such incidents. **Risk Exposure** / **Root causes** Risk that incident management is not effective. / Failure adequately to record remedial actions to address security incidents. **Probability** | **Financial** | **Reputational** | **Operational** | **Legal** | **Rating** Probable | Negligible | Probable | Minor | Negligible | 5:8	Low	Management will ensure that all security incidents, including their remediation actions, are fully recorded within the incident management system. **Responsible Officer:** DISG Apps and Data **Implementation Date:** 31 May 2019
6	**Missing control** We noted that there is currently no practical	No	-	Given the number of sites in use, failure to identify such sites may result in a failure to target particularly 'risky' sites for scrutiny, leading in turn to data leakage and consequent prosecution and reputational damage.	Low	Management should consider adding to the list of sites a data item indicating the presence of

<table>
<tr><th>Ref</th><th>Control</th><th>Adequate control design (yes/no)</th><th>Controls complied with (yes/no)</th><th>Audit findings and implications</th><th>Priority</th><th>Action for management</th></tr>
<tr><td></td><td>means of identifying which SharePoint sites contain personal or sensitive data. Such sites may require particularly robust control over permissions and/or more frequent security auditing.</td><td></td><td></td><td>
<table>
<tr><th colspan="3">Risk Exposure</th><th colspan="3">Root causes</th></tr>
<tr><td colspan="3">Risk that failure adequately to scrutinise “sensitive” sites adequately will lead to data leakage and reputational damage.</td><td colspan="3">Failure adequately to identify sensitive SharePoint sites.</td></tr>
<tr><th>Probability</th><th>Financial</th><th>Reputational</th><th>Operational</th><th>Legal</th><th>Rating</th></tr>
<tr><td>Probable</td><td>Negligible</td><td>Probable</td><td>Minor</td><td>Negligible</td><td>5:8</td></tr>
</table>
</td><td></td><td>data falling into the Top Secret, Secret and Official – Sensitive classifications, and reviewing the security of these sites centrally and/or more frequently.

Responsible Officer:

Data Protection Officer

Implementation Date:

30 September 2019</td></tr>
</table>

APPENDIX A: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The internal audit assignment has been scoped to provide assurance on how the organisations manages the following risk.

Objective of the area under review	Risks relevant to the scope of the review	Risk source
To consider the risks to the security of the information held in SharePoint and propose controls (process, people and tools) to treat the most important.	Strategic risk 6993: Delivery of ICT Change Programme	Strategic risk register

2.1 Scope of the review

In advance of moving data from an existing self-hosted SharePoint infrastructure to an Office 365 cloud-based SharePoint infrastructure, North Yorkshire Police require confidence in their current security policies and data management practices. The intended migration is due in mid-2019 as part of the National Enabling Programme.

This review will focus on the current risks relating to in how SharePoint is used and the management controls to minimise data leakage. This will include a review of sensitive personal data to ensure a least privilege model is adhered to.

SharePoint areas within scope include:

- Corporate Intranet – The 'source';
- Applications – site data lists and workflows; and
- End users – Sites, subsites and shares.

We shall review and assure the controls in place and where possible identify any gaps where additional benefit may be gained through implementing additional controls or procedures

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

SharePoint Governance

A review of the governance, policies and controls over the management and access to information, covering:

- Governance plans;
- Policies / processes defining user group creation; granting user permissions;
- Staff education and training in SharePoint according to assigned role; and
- Communication channels to those who create / modify user groups and permissions.

Data Management

A review of how data is classified and controlled, covering:

- Policies and procedures over data:
- Data sensitivity and segregation; and
- The content types and organisational taxonomies applied.

Managing User Access / Privileges

An assessment of the controls and tools surrounding access to SharePoint sites including:

- Restrictions on access to site administrative accounts or delegated administration;
- Password rules for end user and administrative accounts;
- Who has current access to sensitive data;
- How permissions are granted;
- What activities are performed on the site / content and who is authorised to perform them;
- Extent of permissions for internal users and groups; and
- Orphaned users.

Remote Access / External Sharing:

An assessment of the controls focussing on:

- Top-level security configuration for all sites;
- Rules around remote and third-party access to network;
- Extent to which external sharing is active; and
- Extent to which guest links are used.

Incident Management Reporting:

An assessment of the controls for identifying and reporting security events:

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

Audit Reporting

A review of the level of reporting and analysis of SharePoint user and administrative activity.

The following limitations apply to the scope of our work:

- 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 SharePoint 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 North Yorkshire Police 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 will be on a sample basis for the current financial year only.

- We will not perform penetration testing or vulnerability assessments. The review will be limited to identifying the existence of controls in the areas for review and obtaining supporting documentation.
- Our work does not provide any guarantee against errors, loss or fraud or provide assurance that error, loss or fraud does not exist.

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit:

- Applications and Data Manager
- Temporary Policing Systems Team Leader
- Senior Application Development and Support Engineer

Documentation reviewed during the audit:

- Information Security Policy, v.7
- Internet and Email Policy, v.4
- IAO Handbook, v.3
- Records Management Policy, v.2.1
- Intranet high-level plan
- Senior Application Support Engineer job description (current)
- Site Owner Guide (current)
- The Source User Guide (current)
- Protective Marking scheme v.3.2
- IT Risk Register
- GIRR IT Health Check v.1

FOR FURTHER INFORMATION CONTACT

Dan Harris, Head of Internal Audit

Tel: 07792 948767

Daniel.Harris@rsmuk.com

Angela Ward, Senior Manager

Tel: 07966 091471

Angela.Ward@rsmuk.com

Philip Church, Client Manager

Tel: 07528 970082

Philip.Church@rsmuk.com

rsmuk.com