Internal Audit Report – FINAL

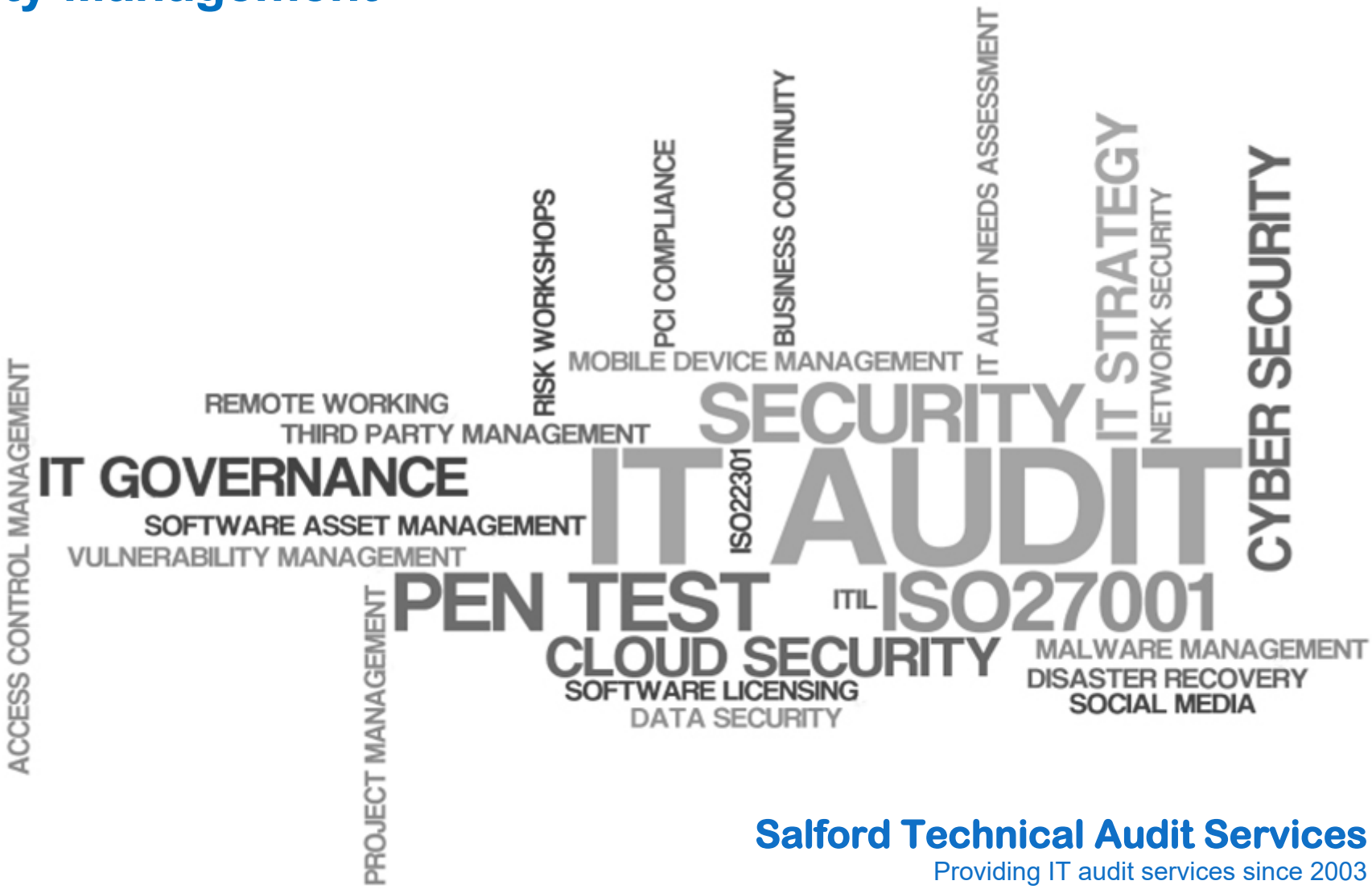
APPENDIX C

Chorley Council and South Ribble Borough Council

Vulnerability Management

April 2024

Version 1.0



Salford Technical Audit Services

Providing IT audit services since 2003

Internal Audit Team and Key Contacts

Client Lead – Internal Audit	Dawn Highton – Head of Internal Audit		
Client Lead - ICT	Jane Norris – ICT Manager Paul Moody – Senior Network Officer, Jason Donnelly – Cyber Security Officer		
Report Author	Owen Griffiths	Client Technical Audit Manager	owen.griffiths@salford.gov.uk
Reviewed By	Gary Marland	Head of Technical Audit	gary.marland@salford.gov.uk

Audit Overview

Overview

Vulnerability management involves the identification, classification, prioritisation, remediation, and mitigation of software vulnerabilities that could be exploited by threats to gain unauthorised access or cause harm. This includes inadequate password management, inappropriate access to files, weak cryptography, and mis-configured applications. It is important to identify and address vulnerabilities through security measures to minimise the risk of exploitation.

Patch management forms a crucial part of vulnerability management and revolves around the installation of vendor released fixes for known vulnerabilities in operating systems and software.

Without good vulnerability management practices, the council is exposed to risks including data breaches and unauthorised access, malware, and ransomware attacks, as well as human error and insider threats. These risks significantly increase the likelihood of legal repercussions, system disruptions, and the compromise of sensitive information.

Audit Objectives

The objective of this review was to verify whether there are appropriate controls in place to minimise the key risks associated with vulnerability management.

The audit concentrated on the following areas:

- Policy and Management Reporting
- Identification, classification and prioritisation
- Remediation (inc. patching)
- Awareness Training

Background Information

Chorley Council and South Ribble Council have merged their ICT departments in recent years. There has been a high level of staff turnover within ICT and difficulty in recruitment to fill vacancies. As a result, there have been numerous delays in projects to improve the vulnerability management infrastructure and processes within the councils.

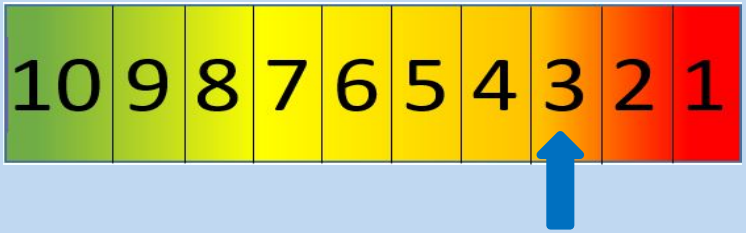
Opinions and Approach

Any opinions and actions arising from the review will be based on interviews with key staff, an evaluation of the documentation in place and observations made when assessing systems and procedures.

Internal Audit performs its work in accordance with its Charter, the Public Sector Internal Audit Standards, and Code of Ethics.

The auditors are alert to indicators that fraud, corruption or bribery may have occurred and consider procedural weaknesses / opportunities that could increase the risk of occurrence. In the event that any concerns were identified, they will have been discussed with management, and reflected in the report detail and action plan. There were no impairments to the independence and objectivity of assigned auditors in relation to the work to be undertaken.

Executive Summary

Risk Opinion	Risk Opinion Score
The review of the councils' vulnerability management concluded that there is no formal vulnerability management process in place. It is acknowledged that patching is performed which mitigates some elements of risk, however, both councils are exposed until vulnerabilities are appropriately managed. It is acknowledged that since the merger of the ICT service covering both councils, there has been a high turnover of staff and filling of vacancies has been a challenge. This has hindered the ability to manage vulnerabilities effectively. As a result, there are three priority 1 and four priority 2 recommendations that if implemented should enhance the current control environment.	 The scale above is an indication of the level of control measures in place to manage risk. See Appendix B for more details.

Scope/Objective	Recommendation Reference[1]		
	1	2	Advisory
Policy and Management Reporting	R1	R2	N/A
Identification, classification and prioritisation	R3, R5	R4	N/A
Remediation (inc. patching)	N/A	R6, R7	N/A
Awareness Training	N/A	N/A	N/A
Total	**3**	**4**	**0**

[1] See Appendix B for more detail on the Recommendation priorities.

Summarised Findings and Actions Required

Objective Area: Policies and Management Reporting

Findings	Recommendation	Priority* (1,2,Advice)	Management Response
There is not currently any approved cyber strategy or vulnerability management process in place, although there are technical controls in place to mitigate core vulnerabilities through patching. However, they are not conducted in a way that can be easily managed or reported and are installed in a mostly manual process. There is no clear reporting of the success or failure of patch installations and as such there is a level of unmanaged risk. The discussions held with ICT staff at the council determined that there were numerous goals that they wished to achieve, and had planned, in order to improve vulnerability management, however, it has currently stalled due to a lack of resource and staff in management positions. **Conclusion:** Without a strategy, the council lacks clear direction, coordination and resources to effectively identify, and respond to cyber risks, potentially resulting in data breaches, system compromises and financial losses.	**R1:** The council should produce a cyber strategy to cover corporate risks regarding cyber security. The council should ensure vulnerability management is included, detailing what needs to be implemented and when in order to provide the greatest level of risk management. This should include vulnerability scanners, automated patching systems, procurement requirements for third parties etc.	P1	Response: Agreed. Responsible person/title: Claire Beattie Timescale: December 2024

The draft patching policy has been reviewed. It contains the key aspects of patch management within the policy that will assist the council in managing vulnerabilities effectively. It specifies requirements for the various IT systems, emphasising the need for up-to-date firmware, OS, and applications, along with the removal of support for obsolete devices. The timelines for patch deployment, based on severity levels, is currently incomplete. A decision is outstanding to state the timeframes and to ensure they a aligned to industry practice. There are separate timings for emergency patching, however, the response times have yet to be completed on the draft policy. ICT have stated that these patches are installed within 72 hours. **Conclusion:** Without clear guidelines on patch management, the council will lack consistency and efficiency in applying necessary updates, leaving systems vulnerable to exploitation and hindering timely response to emerging threats.	**R2:** The policy should be completed and finalised as soon as possible. In order to reduce the administrative burden for ICT staff for patching end user devices, management should explore the possibility for an automatic release of all patches without prior approval. The potential adverse effects of a patch are likely to be less risky than if the vulnerability is exploited. .	P2	Response: Agreed. Responsible person/title: Claire Beattie Timescale: September 2024
The council has a comprehensive Information Security Framework document that is issued and is required to be followed by all employees. Although it does not specifically cover vulnerabilities and patching, it does cover users' responsibilities with regards to notifying ICT of viruses/malware, as well as the importance of remaining vigilant to reduce the chance of	No action required.		

introducing vulnerabilities via downloading or installing unauthorised software. **Conclusion:** Staff should be aware of their responsibilities for avoiding common pitfalls that could impact the security of the corporate infrastructure.			

Objective Area: Identification, classification, and prioritisation			
Findings	**Recommendation**	**Priority*** (1,2,Advice)	**Management Response**
A change management board does not currently meet at the council primarily due to resourcing issues. A Change Advisory Board (CAB) plays a critical role in evaluating proposed changes to IT systems, including patches for vulnerabilities. When discussing vulnerabilities, the CAB should follow a structured approach to ensure thorough assessment and decision-making. **Conclusion:** Without a CAB, changes could be implemented without proper oversight causing adverse effects to systems or introducing vulnerabilities.	**R3:** A CAB should be formed and meet regularly and include the following aspects: • Describe each vulnerability and its severity. • Provide brief details on affected systems and potential exploits. • Evaluate risk based on severity and exploitability. • Discuss available patches, workarounds, and mitigations. • Evaluate feasibility and effectiveness of each option. • Reach consensus on an action plan. • Document decision and assign responsibilities. • Set timeline for implementation. • Review implementation.	P1	Response: Agreed In progress with a meeting arranged for every Thursday and includes change management as an agenda item. Group consists of: Asim Khan Claire Beattie Jane Norris Steve Lyons Katrina Sykes Jason Donnelly New Helpdesk manager Responsible person/title: Claire Beattie Timescale: June 2024

The council has access to Microsoft's Secure Score that can help the council assess and improve their security posture within Microsoft 365 environments, but the information provided is not currently used. It provides a security posture score out of 100 which can increase and decrease based on numerous factors including missing patches, intrusion prevention systems in place and email filtering systems etc. Administrators can use this system to compare their own score to those of similar sized organisations and also add any third-party tools they use as an external mitigation to risks in order to increase their score. For example, the council's Mimecast system for email. By not utilising it, the council is missing out on recommendations for enhancing the security of its cloud-based infrastructure, including email, filtering and tools. **Conclusion:** The secure score is a valuable tool that can provide useful insight into infrastructure health without any additional licencing costs.	**R4:** The council should adopt Microsoft Secure Score as part of a cyber strategy and implement any amendments with a view of improving the score.	P2	Response: Agreed. Product is included within licence agreement and therefore will be evaluated and considered for use going forward. Responsible person/title: Claire Beattie Timescale: September 2024
The council does not currently have a vulnerability scanner which is a fundamental tool for identifying weaknesses and security flaws within the council's IT systems and applications. **Conclusion:** Without this tool in place, the council is exposed to risks of cyberattacks, data breaches, and potential compliance issues.	**R5:** The council should implement a robust vulnerability scanner solution. The tool will enable the council to proactively scan and assess its IT infrastructure for known vulnerabilities, misconfigurations, and other security weaknesses. By regularly scanning and identifying vulnerabilities, the council can take	P1	Response. Agreed This will be implemented as per recommendation. Responsible person/title: Claire Beattie Timescale: September 2024

	prompt remedial actions to mitigate risks and enhance its overall cybersecurity posture. As well as scanning, the software should allow any discovered vulnerabilities to be managed and distributed to relevant staff for remediation or acceptance. This could be managed and raised with in the vulnerability scanner software or passed through to the service desk as tickets as this will allow continuous monitoring of services. In order to reduce licencing costs and for practicality purposes, a sample of end user devices can be scanned and used to determine the likely state of all other end user devices. This should be accomplishable due to the thin-client nature of end user devices.		

Objective Area: Remediation (inc. patching)			
Findings	**Recommendation**	**Priority*** (1,2,Advice)	**Management Response**
Patches are installed on systems regularly to reduce the risk of exploitation of vulnerabilities. They are installed firstly on a few servers deemed less critical in advance of wide-spread installation to ensure that any significant adverse effects would not impact the entire corporate estate. Discussions with ICT staff determined that patches are, however, installed in a timely manner with an expedited installation process for emergency/critical patches. The manual installation process of server patching currently undertook is resource intensive compared to an automated solution and lacks an overarching management view. End user devices consist of thin clients of various configurations. They are patched and updated via the release of updates from Dell which, depending on the configuration of the end user device, can be either monthly or quarterly. The frequency is out of the hands of the council's ICT. In a small number of cases, laptops are part of Microsoft InTune and the underlying Windows operating system is patched, however, all end users must connect to the Citrix client and have no access to the underlying machine. The thin-client nature of end user devices allows updates to be managed centrally, as well as ensuring users have	**R6:** An automated patching solution should be put in place for servers in order to both reduce the staff resource for patching systems and allow the production of KPI data and metrics for management oversight.	P2	Response Agreed This will be implemented as per the recommendation Responsible person/title: Claire Beattie Timescale: September 2024

no ability to install software, reducing the risk of unauthorised software being installed that could take advantage of system vulnerabilities. **Conclusion:** Regular patching of systems with expedited installation for critical patches, lowers the risk of exploitation. However, manual server patching is resource-intensive and lacks centralised management. The highly controlled nature of the thin client devices reduces the risk of introduction of malware or accidental introduction.			
Evidence has been seen of the discussions with third parties arranging the patching of systems out of the control of the council. This has included the agreement of the maintenance window with the supplier as well as the details of the patch to be installed and the approval of council staff for this patching to be undertaken. Although this shows that there is an approval process and agreed scheduling, the information about this change was held within emails which could subsequently be lost should problems arise in the future. **Conclusion:** Third party systems are managed by vendors, however, they are not conducted in a manner that can later be easily traceable.	**R7:** Third-party changes should be included in the CAB mentioned in **R3** to ensure that the details and authorisation of externally managed changes are traceable.	P2	Response - Agreed. This will be implemented as per the recommendation Responsible person/title: Claire Beattie Timescale: June 2024
For third parties that require access to systems in order to manage patches under their control, the council provides an account that also requires multi factor authentication (MFA) in order to reduce the risk of credential theft and access to an attacker who may then introduce malware etc.	No Action Required		

In addition, the user accounts for suppliers are set to be disabled the day after their work is due to complete, preventing user accessing outside of any authorised period. **Conclusion:** Third party access to systems is controlled to reduce the risk of unauthorised access that could lead to malware infection.			

Objective Area: Awareness Training			
Findings	**Recommendation**	**Priority*** (1,2,Advice)	**Management Response**
Audit has experienced ICT and staff's awareness and response to potential vulnerabilities first hand whilst conducting a phishing simulation. In addition to ICT staff managing service desk calls and escalating to management as soon as the issue was noticed (the service desk was initially unaware of the phishing test), they were quick to react and knew how to deal with the issue before being instructed not to react due to it being a test. Numerous staff had called or physically turned up to ICT enquiring about the dubious nature of the email showing that there is a level of security awareness amongst staff although this had yet to be formalised into an online training module. Staff training has increased since the phishing testing and more modules are introduced to the online training platform as well as in-person courses for those staff that fail any training or phishing simulations. **Conclusion:** The risk of users not informing ICT of potential threats is reduced.	No action required.		

Appendix A: Risk opinion score definitions

Risk Opinion Score	Rationale
The risk opinion score reflects how well risks are managed in the area under review and is based on the auditor's judgement taking in to account the number/priority of recommendations made and the overall level of risk exposure including the impact on the organisation as a whole. No scientific formulae can be applied as some areas/objectives may be considered to have a higher weighting factor over other areas/objectives.	
8-10	The range of scores indicate that the controls in place are very effective. Rarely will an auditor award a score of 10 as this would indicate that all risks are being managed effectively and there are no control issues to report.
5-7	The range of scores indicate that the controls in place are reasonably effective.
3-4	The range of scores indicate that the controls in place are limited in their effectiveness.
1-2	This range of scores indicate that the level of control in place is minimal. If necessary, we may request that the executive management team assess the potential impact on the organisation and take urgent action.

Appendix B: Recommendation priority definitions

Recommendation Priority	Rationale
1	The recommendation is **essential** to the management of risk within the area under review.
2	The recommendation is **important** to the management of risk within the area under review.
Advisory	This is a suggestion intended to enhance the existing management of risk within the area under review.

Proprietary Information