ICT Server Administration & Security

City of York Council

Internal Audit Report 2019/20

Business Unit: Customer and Communities
Responsible Officer: Director of Customer and Communities
Service Manager: Head of ICT
Date Issued: 12 May 2021
Status: Final
Reference: 10270/002

	P1	P2	P3
Actions	**0**	**1**	**3**
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

Information is one of the most valuable assets held by any organisation. To ensure the ongoing provision of council services, it is vital that access to, and security of, network services and data is maintained.

The key hardware supporting the services provided by City of York Council is located in a dedicated data centre at West Offices, with a secondary facility at the Hazel Court Eco Depot.

Weak physical, environmental or logical security arrangements could lead to unauthorised access to data or loss of service availability. Therefore, this audit reviewed the arrangements in place for securing the council's servers and monitoring server performance.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system will ensure that:

- The council's data centres are only accessible by authorised personnel.
- The council's data centres are protected by environmental controls.
- The council's servers are securely configured to reduce the potential points of attack.
- The performance of the council's servers is closely monitored to ensure that they are meeting the demands of end users.

Contact with officers was ceased in March 2020 to enable local authorities to focus their efforts on managing the rapid changes announced by central government in relation to the Covid-19 outbreak.

The following findings are identified from a limited range of testing arising from information and supporting documentation accessed prior to 25 March 2020. We could not determine if access to the data centres was restricted to authorised personnel and if there were change management controls in place. Contact was resumed with officers in April 2021 to confirm the findings raised and to agree actions.

Key Findings

Based on the testing that could be completed prior to the Covid-19 pandemic, it was found that there are suitable controls in place to secure servers against physical and logical attacks. There are also suitable arrangements to monitor server performance and control the data centre environment.

The council's servers are securely configured to reduce potential points of attack. There are suitable malware monitoring and intrusion detection and prevention systems in place, as well as a routine patching cycle. However, testing regarding any exceptions to the patching routine was not completed due to Covid-19.

The council uses SureCloud to scan for vulnerabilities on a weekly basis so that these can be resolved. However, review of a report of known vulnerabilities with a CVSS score of 6.8 or higher dated 26 March 2020 found that more than 10% (84 of 795) of them had been known to the council for more than a year. The reasons for this are varied; some vulnerabilities may be related to unsupported legacy systems, while in other cases the council may be waiting for a supplier to provide a solution. The council has implemented compensatory control measures, such as virtual patching and extended support from Microsoft for legacy systems, to reduce the risks associated with these vulnerabilities.

Backups are taken periodically, but it was not confirmed whether these are tested to ensure they can be restored. Servers are built using server templates based on Microsoft settings. This enables quick deployment of secure servers. Server performance is monitored using LogicMonitor, which is a comprehensive and highly customisable system.

Access to servers and privileged accounts should be conducted via secure jump servers, but it is possible to circumvent this requirement. Direct access to servers is needed for certain administrative functions that cannot be completed via a jump server. All access attempts are logged, but at the time of the audit they were not actively reviewed to identify routine breaches of procedure or unusual access attempts. Since completion of the audit, officers have implemented a system to provide monthly reports of all access attempts so that these can be reviewed and investigated if needed.

ICT policies are held on the intranet, while procedure documentation is held in an online database or ICT work folders. Discussion with officers and review of the documents found that some require review.

A walkthrough test of the data centre at West Offices was conducted with the Data Centre Technician, but a similar test was not conducted at Hazel Court due to Covid-19. The physical control measures were discussed with the Gough & Kelly Senior Operations Manager, but compliance testing to confirm the effectiveness of the controls was not completed. It was noted that data centre access procedure documents were overdue for review. The annual deep-clean of the data centre had been delayed due to planned maintenance work. Overall, the physical and environmental control measures described by officers and witnessed by the auditor appear to be appropriate.

Overall Conclusions

A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1 Monitoring of access to privileged accounts via jump servers

Issue/Control Weakness	Risk
Audit logs of access attempts to privileged accounts and servers are not reviewed.	If audit logs are not reviewed, routine breaches or unusual access attempts may not be identified and investigated.

Findings

It is a requirement that access to privileged accounts and servers for administration is carried out via secure 'jump' servers. However, it was found that this is not rigidly enforced and, although all access is logged, audit logs are not reviewed.

ICT use purpose-built jump servers to provide an additional layer of security when accessing privileged accounts. ICT system administrators are required to use these servers when accessing privileged accounts or other servers because they provide a higher level of security. However, it is still possible to access privileged accounts and servers without using the jump servers because ICT did not want to lose access to privileged accounts and servers in the event of an emergency. Direct access to servers is also needed for certain administrative functions that cannot be completed via a jump server.

To mitigate this weakness, all access attempts are recorded, whether they are made via a jump server or not. However, it was found that the audit logs are not reviewed to identify routine breaches of this procedure or unusual access attempts.

Agreed Action 1.1

Since the audit, ICT have implemented a system that provides a monthly report of usage of infrastructure and database administrator accounts. This is automatically sent to the ICT Infrastructure Manager and Infrastructure Services Team Leader for review and investigation of any unusual activity.

Officers are investigating a new approach to accessing servers known as 'browse down', which is recommended by NCSC. A pilot will be carried out during 2021 and a decision made on whether or not to roll this out to all servers across the council.

Priority	2
Responsible Officer	ICT Infrastructure Manager
Timescale	30 November 2021

2 ICT policies review and availability

Issue/Control Weakness	Risk
Some ICT policies are overdue for review or are not available on the intranet.	If policies are not up to date or available, they may not be followed correctly.

Findings

During the audit, policies for acceptable use, vulnerability management and change management were reviewed.

It was found that the Information Systems Security & Acceptable Use policy and the ICT Vulnerability Management policy available on the intranet were both dated to June 2018 and were thus overdue for review. The Change Management policy was not available on the intranet, but a copy dated to July 2017 had been provided to Internal Audit during a previous audit. Policies should be reviewed to ensure they are up to date.

Agreed Action 2.1

ICT policies are currently under review in conjunction with the Yorkshire & Humber WARP group.[1] Policies will be reviewed, updated and placed on the intranet using 'Markdown' text, which will make them more accessible and fully searchable by users.

Priority	3
Responsible Officer	ICT Infrastructure Manager
Timescale	31 July 2021

[1] WARP is the Warning, Advice and Reporting Point where members can receive and share up to date advice on information security threats: https://www.ncsc.gov.uk/information/what-warp

3 Procedure documentation for server rooms, servers and applications

Issue/Control Weakness	Risk
Some procedure documentation for data centre access, servers and applications are out of date.	Out of date documentation could lead to procedures for accessing data centres and configuring or maintaining servers and applications being followed incorrectly.

Findings

The audit identified a number of procedure documents that are due for review.

There are documented procedures for access to the data centres at West Offices and Hazel Court. However, it was noted that the procedure documents were due for review in June 2019 but have not yet been reviewed. Furthermore, officers stated that access rights are reviewed quarterly by the ICT Infrastructure Manager to ensure access is still appropriate, with the list provided by Gough & Kelly. However, this control is not recorded in the procedure documents.

Procedure documentation (also known as 'build' documentation) for servers and applications are held by ICT in the Domain Services Documentation folder or on Confluence Knowledge Base, an online system. These cover such topics as configuration, troubleshooting and maintenance tasks.

Review of these documents and discussions with the Infrastructure Services Technical Team Lead found that some documents may be out of date due to changes made by suppliers or the retirement of particular products (e.g. it was noted that Exchange Server 2007 documentation is still held, although it is no longer in use).

Agreed Action 3.1

Since the audit, the data centre access procedures have been reviewed and are available on the council's intranet.

Other procedure documentation will be reviewed and updated as required.

Priority	3
Responsible Officer	ICT Infrastructure Manager
Timescale	31 July 2021

4 Server room deep clean

Issue/Control Weakness	Risk
The annual deep clean of the West Offices data centre has been delayed due to planned maintenance work.	If the data centre is not kept clean, dust and dirt may accumulate that could affect the smooth functioning of equipment.

Findings

Officers stated that annual deep cleans are undertaken in the West Offices data centre to prevent accumulation of dust or dirt that could affect the functioning of ICT equipment. However, at the time of the auditor's walkthrough of the data centre (26 February 2020), the deep clean had not been completed.

The Data Centre Technician stated that the deep clean for 2019/20 had been delayed because there was maintenance work scheduled in the data centre. As this work might create additional dust and dirt, it had been decided to delay the deep clean until the work had finished so that the deep clean would not have to be repeated.

While the reason for delaying the deep clean is valid, officers should ensure that the deep clean is carried out as soon as is practicable once the maintenance work has been completed.

Agreed Action 4.1

The Covid-19 pandemic has further delayed the data centre deep clean. The deep clean will be rearranged and carried out as soon as possible.

Priority	3
Responsible Officer	ICT Infrastructure Manager
Timescale	31 July 2021

Audit Opinions and Priorities for Actions

Audit Opinions

Our work is based on using a variety of audit techniques to test the operation of systems. This may include sampling and data analysis of wider populations. It cannot guarantee the elimination of fraud or error. Our opinion relates only to the objectives set out in the audit scope and is based on risks related to those objectives that we identify at the time of the audit.

Our overall audit opinion is based on 4 grades of opinion, as set out below.

Opinion	Assessment of internal control
Substantial Assurance	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited Assurance	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

Priorities for Actions

Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Veritau

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.