Internal Audit Report

Chorley Council and South Ribble Borough Council

Physical Security and Environmental Controls

Date October 2023

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 Audit and Risk		
Client Lead - ICT	Emma Marshall – Head of ICT		
Report Author	Angela Fletcher	Client Technical Audit Manager	angela.fletcher@salford.gov.uk
Reviewed By	Gary Marland	Head of Technical Audit	gary.marland@salford.gov.uk

Audit Overview

Overview

Chorley Council and South Ribble Borough Council have a shared ICT service, supported by three separate data centres and a key comms room.

Robust physical security and environmental controls at all data centres are key to ensuring continuity and availability of data and services.

Inadequate physical security can lead to unauthorised access to critical systems which could lead to loss of service and data.

Additionally, insufficient environmental controls could also affect the availability of the councils' critical IT infrastructure, e.g., fire, flood, power loss.

Audit Objectives

The objective of this review was to verify whether there are appropriate controls in place to minimise the key risks associated with the management and operation of the councils' data centres.

The audit concentrated on the following areas:

Physical Security

- Perimeter Access
- External and Internal Access Controls
- CCTV

Environmental Controls

- Fire Protection
- Water / Flood Protection
- Environment – Air Quality, Temperature, Sound level.
- Cooling
- Power / Electrical Protection
- Equipment Positioning / Flooring

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 Physical Security and Environmental Controls for the Chorley and South Ribble data centres and comms room concluded that key risks are not being mitigated to an acceptable level. There are significant concerns regarding several critical areas, including unauthorised physical access, absence of internal CCTV surveillance, deficient fire suppression systems, power protection and water ingress risks, all of which have reflected the lower risk opinion score. The consequence of failing to mitigate these significant risks could lead to both councils losing critical IT services. Following this review, it is advised that an urgent assessment of the recovery timeframes of key services must be formally assessed should the data centres not be available. As a result, we have made eleven priority 1 recommendations and one advisory point that, if implemented, will 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
Perimeter Access	R1	-	-
Access Control Systems	R2	-	-
Visitor Management	R3	-	-
CCTV	R4	-	-
Fire Detection and Suppression Systems	R5	-	-
Water/Flood Protection	R6	-	-
Environment – Air Quality, Temperature, Sound Levels	R7	-	A1
Cooling	R8	-	-
Power/ Electrical Protection	R9 and R10	-	-
Equipment Positioning/ Flooring	R11	-	-
Total	**11**	**0**	**1**

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

Summarised Findings and Actions Required

Objective Area: Physical Security

Findings	Recommendation	Priority* (1,2, Advice)	Management Response
Perimeter Security All data centres are discreetly located across various council owned buildings. None of the data centres display visible signage indicating their purpose. For ease of reporting, Chorley's data centres are referred to as DC1 and DC2, and South Ribble's data centre is referred to as DC3 and a key comms room is referred to as CR4. It is acknowledged that there are plans to close DC2 and existing equipment will be relocated. (NB: Timescales not known) Perimeter security is provided by CCTV surveillance systems which monitor the outer premises and entry points to the buildings. The data centres are in strong building structures which provide security against unauthorised physical access attempts. DC3 features high-level windows equipped with blinds, ensuring no visibility from the outside. However, none of the data centres have intrusion detection systems in place. **Conclusion:**	**R1** - Management should implement intrusion detection systems at all data centres to enhance security against unauthorised physical access.	P1	Response: Agreed to implement recommendation. Responsible person/title: Head of Property and Development Timescale: 31st March 2024

The risk of unauthorised physical access to the data centres is increased due to the absence of intrusion detection systems.			
Access Control Systems Of the 4 rooms visited only two operate a secondary access control for enhanced security. • DC1 - IT staff require an office access pass to enter a dedicated room followed by keys from the civic team to access the data centre itself. However, there is a significant control gap as the team hand out the keys without verifying the identity of the recipient. • DC3 - IT staff need an office access pass to first enter an intermediary room after which a generic code, known solely to IT personnel, is used to access the data centre itself. • DC2 and CR4 rely solely on single-factor authentication using office access passes. **Conclusion:** The risk of unauthorised access is increased, where access is a single access control point.	**R2** - Management should install a secondary access control security feature, either through a physical lock or ideally using an additional biometric access control system (face or fingerprint), that will also provide increased tracking of access. A register of authorised users and a log should be maintained in DC1 to enhance the control over access.	P1	Response: Agreed to implement recommendation. HFX Door entry system to be used where appropriate. Responsible person/title: Head of Property and Development Timescale: 31st March 2024
Visitor Management DC1 and DC2 have no formal visitor access procedures in place. There have been several occasions where Property Services have provided maintenance contractors with access to DC1, without notifying the IT department, which resulted in contractors being left unsupervised. Visitors to DC3 are accompanied and supervised, however, visits are not logged. CR4 is shared with DWP	**R3** - Management should implement formal visitor management procedures, including access requests, sign-in/out processes and robust identification verification. Visitors should be accompanied by authorised IT personnel at all times and regular audits of access logs should be undertaken to enhance	P1	Response: Agreed to implement recommendation Responsible person/title: Head of Property and Development

and operates an appropriate visitor access request procedure which ensures visitors are always supervised. **Conclusion:** The risk of a security incident as a result of unauthorised or unsupervised access is increased due to the lack of formal visitor management procedures and insufficient oversight of visitor activities within the data centres.	security of the data centres and the data held within them.		Timescale: 31st December 2023
CCTV None of the data centres/comms rooms have CCTV cameras installed. This absence means that while external areas might have some level of surveillance, the internal parts of the data centres remain exposed. **Conclusion:** The lack of CCTV cameras within the data centres increases the risk of unauthorised access and security breaches.	**R4** - Management should install CCTV cameras in all sensitive rooms and ensure they feature active monitoring and real-time alerts to improve security through prompt threat detection and response.	P1	Response: Agreed to implement recommendation Responsible person/title: Head of ICT Timescale: 31st December 2023

Objective Area: Environmental Controls			
Findings	**Recommendation**	**Priority*** (1,2, Advice)	**Management Response**
Fire Detection and Suppression Systems Several concerns are noted regarding the fire detection and suppression systems across the data centres: • While all data centres are equipped with fire suppression systems, only DC3 has an Alert Management System for critical temperature notifications. • DC1 staff are untrained in the proper use of their fire suppression system, endangering infrastructure and potentially lives. • Flammable materials are stored near DC1. • DC2 has insufficient fire suppression measures and noted cable damage due to rodents. • Fire suppression cylinder stretch tests for DC3 and CR4 are urgently due, with current certifications expiring in November 2023. **Conclusion:** The risk of fire damage is significantly increased as a result of the concerns raised above.	**R5 -** Management should swiftly address the highlighted concerns. This includes offering comprehensive fire suppression training for key IT staff, regular maintenance and testing of fire suppression systems, including required stretch testing of canisters and removing any combustible materials stored nearby. It is strongly advised that all data centres fire suppressant systems should be linked to an effective environment alert management system, that can send audible alarms both internally to IT rooms and alerts via emails and text to key on call staff.	P1	Response: Agreed to implement recommendation Responsible person/title: Head of Audit and Risk Timescale: 31st December 2023 Response: Agreed to implement recommendation Responsible person/title: Head of Property and Development Timescale: 31st March 2024

Water/Flood Protection There are no water ingress detection systems to identify potential water intrusion in any of the data centres. • There are concerns about damp-proofing of DC1 which is situated in a basement. • There is an inherent problem of water ingress into a basement room adjacent to DC1. Sandbags are positioned at the door as a way of protecting DC1 from the water ingress. • Servicing of the air conditioning at DC2 resulted in a significant water leak that went undetected for two days. • There are toilets situated directly above DC2 and a water pipe located directly above DC1 creating additional water-related risks. • While the DC3 offers some protection from flooding with its raised floor, comprehensive water diversion measures to safeguard critical areas and infrastructure are insufficient. **Conclusion:** The risk of flooding in the data centres is increased as a result of the issues highlighted above.	**R6 -** Management should consider installing water ingress detection systems in all data centres and have them linked to an effective environment alert management system. This will provide an early warning system to allow key IT staff to provide a timely response to either move critical servers or initiate a controlled shut down. Critically the inherent water ingress issue at DC1 should be assessed and rectified at the earliest opportunity. The location of all cooling systems should be evaluated to mitigate the risk of water ingress near any electric system i.e., server racks.	P1	Response: Agreed to implement recommendation Responsible person/title: Head of Property and Development Timescale: 31st March 2024
Environment – Air Quality, Temperature, and Sound Levels All data centres lack systems to monitor air quality or humidity. As none of the rooms are occupied with staff and operate a 'lights out approach', sound risks are not applicable, unless staff are in the rooms for long periods of time.	**R7** - Management should explore the implementation of air quality and humidity alert systems in all data centres to maintain optimal environmental conditions.	P1	Response: Agreed to implement recommendation Responsible person/title: Head of Property and Development

Conclusion: There is a greater risk of inefficiency, higher energy consumption, and potential overheating in the data centres due to inadequate air quality, temperature controls.	**A1** - Risk assessments should be undertaken on the sound levels of the data centres and guidance should be sought on what is considered a safe period of time to remain inside the data centre during servicing and maintenance. It should be noted that ear protection should be worn when operating in areas above 85 dB(A). As the average data centre is over 90dB(A) then ear protection should be available in all rooms.	A1	Timescale: 31st March 2024 Response: Agreed to implement recommendation Responsible person/title: Head of ICT Timescale: 31st December 2023
Cooling We noted the following observations in relation to air cooling: • DC1 maintains its air conditioning at an excessively low temperature, which could lead to higher than necessary costs. • DC2 lacks dedicated cooling, increasing the potential for overheating. • DC3 has a temperature monitoring system, but its alert feature for IT staff about temperature changes is not working. • CR4 utilises a cycling air conditioning system to optimise energy efficiency.	**R8 -** Manufacturers recommended cooling tolerances should be identified and cooling settings should be adjusted and aligned to maximise operational performance and reduce energy costs.	P1	Response: **Action implemented** Responsible person/title: Timescale:

Conclusion: There is a greater risk of overheating and potential fire due to the lack of monitoring of the cooling systems deployed. Also, as energy costs are considerable, cooling rooms at below manufacturers recommended levels will be wasting energy.			
Power/Electrical Protection - UPS DC1, DC2 and CR4 do not have the UPS (uninterrupted power supply) system connected to any environment alert management system, which can result in delays in identifying UPS malfunctions. A concerning observation is that if the DC1 building experiences a power loss, the server room's lighting is compromised, potentially impacting the ability of IT personnel to undertake disaster recovery actions. In contrast, DC3 is equipped with UPS and generator systems that are connected to an environment alert management system. This provides a timely alert via email and text to key IT staff. The DC3 and CR4 UPS and generator undergo annual servicing and tests, which is important for their reliability in critical scenarios. **Conclusion:** Due to the issues highlighted above, there is an increased risk of power disruptions and data loss at DC1, DC2 and CR4.	**R9** - Management should consider connecting the UPS to an environment alert management system to allow early detection of a malfunction. All data centres should have emergency lighting, which can operate during a power outage to enable staff to undertake effective disaster recovery operations.	P1	Response: Agreed to implement recommendation Responsible person/title: Head of Property and Development Timescale:31st March 2024

Power/Electrical Protection – Backup Generators There have been no live tests of the backup generator at DC1 to verify system readiness during critical power interruptions. **Conclusion:** There is an increased risk that power will not continue to be provided to DC1 once the UPS batteries fail (Usually after 30 minutes) should the backup generator fail to operate as expected.	**R10** – Backup generators should be tested at least weekly to ensure that they will effectively operate when required.	P1	Response: Agreed to implement recommendation Responsible person/title: Head of Property and Development / Head of Operational Assets Timescale:31st March 2024
Equipment Positioning/Flooring In most respects, equipment positioning and flooring in the data centres are managed adequately, allowing for optimal airflow and facilitating maintenance of server racks and cable management systems. However, there are a couple of challenges as follows: • DC2, as previously mentioned, faces challenges related to targeted cooling and rodent-related cable damage beneath the floor. • DC2 and DC3 have substantial IT equipment stored within them. This excess storage not only raises concerns about accessibility but also poses potential fire and safety hazards. **Conclusion:** The storage of IT equipment, particularly in DC3 increases the risk of both safety incidents and operational disruptions.	**R11 -** Management should remove the excess IT equipment stored within the data centres to adhere to safety standards, ease access, and reduce the likelihood of operational disruptions.	P1	Response: Agreed to implement recommendation Responsible person/title: Head of ICT Timescale:31st March 2024

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/objective.	
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