CYC Schools Themed Audit - Cyber Security & IT Management

City of York Council

Internal Audit Report 2020/21

Business Unit: People Directorate,
Responsible Officer: Assistant Director, Education & Skills
Service Manager: Head teachers
Date Issued: 14/09/21
Status: Final
Reference: 15699/030

	P1	P2	P3
Actions	**0**	**0**	**6**
Overall Audit Opinion	Reasonable Assurance		

Veritau

Summary and Overall Conclusions

Introduction

Schools must have adequate systems in place to ensure their IT systems are protected and secure, and comply with statutory requirements. Having comprehensive security measures in place helps ensure data, systems and assets are protected from damage, unauthorised access, loss and misuse.

Cyber Security threats to organisations including educational establishment in the UK have recently become more prevalent. Since August 2020, the National Cyber Security Centre (NCSC) has investigated an increased number of ransomware attacks including attacks on schools and colleges. It is that vital schools have robust measures in place to prevent such attacks.

This audit reviewed the Cyber Security and IT management controls in place at CYC maintained schools.

Due to the Covid-19 Pandemic, we were unable to complete actual visits to the schools. Therefore reliance was placed on the responses to questionnaires and a review of the supporting evidence provided. This was followed up with an online meeting where necessary. The audit programme was based on best practice from the ISO 27001, Internet security centre guidance and Global Technology Audit Guide Cyber Security Assessment.

Objectives and Scope of the Audit

The purpose of this audit is to provide assurance to management that adequate Cyber Security and IT management arrangements are in place to ensure

- Appropriate physical securities are in operation.
- There is adequate external assurance that IT systems are secure.
- A firewall is in place and is managed appropriately.
- There are suitable logical access controls.
- Sufficient malware protection is in place and is well managed.
- Patch management is handled appropriately to keep IT assets up to date.
- Plans and procedures to manage disaster recovery and cyber incidences are in place.
- There is effective management of ICT and software assets.
- There is suitable training for all staff with access to IT systems within the school.

The audit covered practices at 9 maintained schools. It did not cover testing of the ICT asset register.

Key Findings

Schools obtain a significant level of IT provision through IT contractors. Of the 9 schools included in the review 2 used SMD as their IT contractor, 1 school used Primary Tech and the remaining 5 Schools used Vital.

6 schools had server rooms on site. Several of these schools had issues relating to physical security of the server room some of which could be addressed easily but others may need further consideration. In particular 3 schools indicated that they had no temperature and humidity monitoring combined with no means of preventing overheating. If the server exceeds the recommended temperature damage may be caused and data may be lost. Two of these schools also had water pipes running through the server room which may increase the risk of humidity issues. Additionally wires in 3 server rooms were not always labelled. Labelling is recommended to ensure efficient operation of the server and may become an issue if the school changes its IT provider. It was also noted that one school had some data cabinets that were not locked or located in a secure area putting the network at risk from vandalism or accidental damage.

All schools purchased broadband and a fully managed firewall service through and SLA with CYC. This SLA also provides independent external assurance that systems are secure through external penetration or intrusion testing.

In general good logical access controls were in place. All schools had an appropriate system for allocating and revoking user accounts, however 2 schools did not ensure that a reconciliation of live user accounts to current staff and pupils was completed and most schools did not retain evidence of this reconciliation. Passwords for the school network were strong and were changed on a regular basis. It was noted however that those schools allowing remote access to the school network did not use 2 factor log. It is advised that this is put in place to provide an extra layer of security. Social media accounts were controlled through appropriate restriction of access to passwords. All schools provided on line learning as required by the DfE accessed by staff and pupils through their school log in. Any live streaming was suitably constrained.

All schools indicated that they had anti-virus software in place (malware protection), adequate patch management procedures with an appropriate patch cycle, and regular back up and testing of network files. These tasks were in the main being completed by the IT contractor but (with the exception of 1 school), no evidence or confirmation of completion of these tasks was obtained. It is recommended that schools ensure they receive evidence form the contractor that these services are being carried out.

Not all schools had an IT Disaster Recovery Plan in place or a clearly documented process for the management of information security incidents. This increased the risk that in the event of a cyber-security incident appropriate action will not be taken promptly and effectively to resolve the incident and to ensure it is reported correctly if required by the ICO.

Good controls were in place to track and account for IT hardware and inventory was maintained of software assets. Back up discs were encrypted and held securely off- site or on site in a fire a flood proof location. There were however some identified weaknesses in relation to the protection of data. Disposal certificates for equipment leased from the IT contractor were not generally requested by the schools therefore the school had no assurance that they have been wiped of data before being disposed of. Also several schools had laptops which

were not encrypted to prevent unauthorised access to data and some schools did not ensure unauthorised IT assets were blocked from the network or set to read only to prevent the unauthorised transfer of data.

Mandatory training for staff in cyber security awareness was not in place at all schools. Acceptable use documentation was in place setting out the restrictions for using IT equipment and the IT network which was acknowledged by both staff and students.

Overall Conclusions

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. Our overall opinion of the controls within the system at the time of the audit was that they provided Reasonable Assurance.

1 Security of Server Rooms and Data Cabinets

Issue/Control Weakness	Risk
The physical security of some server rooms and data cabinets does not meet best practice guidelines	Damage to equipment resulting in the school's data being lost and the network being out of action

Findings

Schools are expected to have suitable physical securities in place to ensure equipment in server rooms and data cabinets are protected from theft, vandalism and adverse operating conditions. The size and layout of some of the schools may mean that it is not always possible to comply with best practice however, it would be beneficial for schools to review where they are below practice and consider if there is a cost effective and practical solution to allow them to reduce risk. 1 school which had several of the issues detailed below was due to move its server room to the CYC data centre in Summer 2021. Of the 6 schools with server rooms on site

- 1 school did not have restricted access to the server room. Only two schools had CCTV in place to monitor access
- 3 schools had no systems in place for monitoring the temperature and/or humidity. These schools also had no means of preventing overheating eg air conditioning. In the event that the temperature or humidity exceeds the server's optimal temperature the server could be damaged Two of these schools also had water pipes running through the server room which further increases the humidity and water damage risk
- 3 schools had unlabelled wires in the server room. Efficient labelling helps to ensure effective server room performance

1 school did not have all data cabinets locked or located in a secure area to prevent unauthorised access (although for one of these schools all the data cabinets were located in the locked server room and were therefore not generally accessible). If the switches within the cabinets were damaged this could lead to unavailability of key systems.

Agreed Action 1.1

The School Business Support Manager will share the control weakness with Schools and will direct them to relevant guidance during Autumn 2021. Schools will need to take responsibility for reviewing the physical server room and data cabinet security in their school building and agree the improvements and funding.

Priority	3
Responsible Officer	School Business Support Manager
Timescale	31 October 2021

2 Contractor Services

Issue/Control Weakness	Risk
The completion of regular IT processes by the school's IT contractor is not evidenced	The IT contractor may fail to deliver the expected services and system security may be compromised.

Findings

All schools are required to have systems in place to complete the following IT functions

- Regular update of anti-virus software protection to detect and remove viruses and other kinds of malicious software
- Update of IT assets and software with the latest patches (these are often virus related and required to fix known issues that cybercriminals are currently exploiting as well as providing performance improvements or new software features)
- Back up to protect data in the event of system failure or file corruption
- Back-ups testing to ensure files can be restored.

These IT functions were in the main carried out by the schools IT contractor and included in the contract specification. However for 8 out of 9 schools evidence to confirm the completion of these processes was not requested. Verification that the contractors are completing these requirements should be part of the contract monitoring procedures.

1 school completed the update of the ant-virus protection and patch management in house, updating both when desktops are updated with a new image. The anti-virus software is currently manually updated however they are currently changing to centralised management.

Agreed Action 2.1

The School Business Support Manager will share the control weakness with Schools and will direct them to relevant guidance during Autumn 2021. Schools will need to take responsibility for contract monitoring of the IT contract and ensure that the contractor provides written assurance (evidence) that they are completing the essential updates, back-ups. The school should keep a record of this evidence.

Priority	3
Responsible Officer	School Business Support Manager
Timescale	31 October 2021

3 User Accounts and Passwords

Issue/Control Weakness	Risk
Issues were identified in relation to the verification of user active accounts and the security of remote log on.	Unauthorised access to IT systems and data

Findings

Schools should have a system in place to reconcile current staff and students to the live user accounts to ensure there is no unauthorised access in place. 2 schools did not have such a system in place and 4 schools did not retain evidence of that this reconciliation is completed.

5 schools allowed remote log in to the schools network but did not require 2 factor authentication as an additional security measure. 2 factor authentication requires a password plus another method to prove your identity (generally a generated code) or access from a specified device and increases the level of security.

Agreed Action 3.1

The School Business Support Manager will share the control weakness with Schools and will direct them to relevant guidance during Autumn 2021. Schools will need to take responsibility for verification of user active accounts and secure remote log in arrangements

Priority	3
Responsible Officer	School Business Support Manager
Timescale	31 October 2021

4 Disaster Recovery and Incident Reporting

Issue/Control Weakness	Risk
In the event of unplanned incidents such as, power outages, cyberattacks, information security incidents and any other disruptive events the school does not have an effective plan of action in place.	Data and functionality may be lost for an extended period and the school may not comply with ICO reporting requirements.

Findings

Schools should have an IT Disaster recovery plan in place which documents the procedure to be followed in order to achieve partially or full restoration of the ICT infrastructure/systems following an outage. The plan should aim for the IT systems within the school to be restored within a predefined time frame. This includes restoring any lost data held in back-up drives. The disaster recovery plan may form part of the schools business continuity plan.

Schools should also have a clearly documented process or policy for the recording and reporting of management information security incidents. This should form part of their information management framework.

- 3 schools did not have an IT Disaster Recovery Plan in place.
- 3 schools did not have a clearly documented process or policy for the management of information security incidents.

Agreed Action 4.1

The School Business Support Manager will share the control weakness with Schools and will direct them to relevant guidance during Autumn 2021. A Model disaster recovery template document will be shared with schools. A data and cyber security breach prevention and management plan will also be shared with schools for them to consider and adapt to meet their needs if required.

Priority	3
Responsible Officer	School Business Support Manager.
Timescale	31 October 2021

5 IT Assets

Issue/Control Weakness	Risk
Practices at some schools may result in data held on IT assets not being sufficiently protected	Data may be stolen from IT assets which aren't encrypted or disposed of in a secure manner

Findings

In order to protect IT assets from data loss it is recommended good practice that all assets which can store data including back up discs and any other removable storage are encrypted. IT networks should also be protected from potential data loss through blocking unauthorised IT assets or setting them to read only. Additionally, IT asset disposal procedures should ensure assets are wiped of all data before disposal, confirmed through the receipt of a disposal certificate. This process is carried out by via the schools IT contractor where equipment is leased from them.

- 4 schools had some laptops which were password protected but not encrypted. The ICO recommends all laptops with data storage are encrypted as password protection does not provide sufficient security.
- 4 schools had not ensured that unauthorised network assets were blocked or set to read only to prevent the unauthorised transfer of data.
- 8 schools stated that a copy of the disposal certificate was not requested by the school when IT assets leased from the IT contractor are disposed of.

Agreed Action 5.1

The School Business Support Manager will share the control weakness with Schools and will direct them to relevant guidance during Autumn 2021. Head teachers and SBM's need to address issues relevant to their schools.

Priority	3
Responsible Officer	School Business Support Manager
Timescale	31 October 2021

6 User Awareness of IT Issues

Issue/Control Weakness	Risk
Some schools do not require staff to complete cyber security awareness training	The school is vulnerable to cyber-attacks which may result in data loss and financial loss to the school and the disruption of education provision

Findings

Schools and their staff need to be aware of cyber risks, how to improve their defence against online attacks including ransomware attacks and how to mitigate the effect of such cyber incidents. Most cyber security incidents are as a result of human error and schools should have robust cyber security training in place for all staff.

Although all schools indicated that staff were made aware of cyber security through policies, induction and bulletins only 4 schools had mandatory logged cyber security awareness training in place.

Agreed Action 6.1

The School Business Support Manager will share the control weakness with Schools and will direct them to relevant guidance during Autumn 2021. A training pack will be shared with schools to adapt and use for training purposes and raising awareness – such as posters to remind staff about what a possible cyber incidents may look like in practice. A discussion about Cyber security has taken place through the SBM meetings, however a follow-up will be arranged in Autumn 2021 with more examples of what can go wrong. Head teachers should arrange a review of their schools Cyber training needs and action.

Priority	3
Responsible Officer	School Business Support Manager
Timescale	31 October 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.