Columbus City Schools
Office of Internal Audit

Office of Technology - Follow-up

Status Report

Report Date: August 29, 2019

Table of Contents

Title	Page
Status Report Overview	3
Executive Summary	4
Summary of Recommendations	6
Summary Charts	8
Details Regarding Recommendations Not Implemented	9

Office of Technology Follow-up Status Report Overview

The initial **Information Technology audit** reports were presented to and approved by the CCS Audit and Accountability Committee on June 17, 2014, March 26, 2015, October 27, 2016, and August 17, 2017. As part of the initial audits, there were a total of 73 **recommendations** that were made for the Office of Technology. The objective of the follow-up review was to ensure Management has taken corrective action to address the outstanding high rated issues identified by the Office of Internal Audit / Schneider Downs & Co., during the initial audits.

73
Total Corrective Action Plans Developed by Management

32
Corrective Action Plans **Implemented** by Management

19
Corrective Action Plans **Not Implemented** by Management

22
Corrective Action Plans **Not Tested** by OIA

Overview

- Written procedures were developed by Office of Technology for job scheduling.
- The Office of Technology removed the last Windows XP machines from the network in November 2018.

Outstanding Audit Issues

- There have been no password requirements set-up for RighTrak (Food Service) or VersaTrans (Transportation).
- The Office of Technology has not performed an annual self-assessment of IT risk.
- The Office of Technology has not officially established an IT Steering Committee.
- The Office of Technology has not implemented an enterprise-wide, comprehensive user access review process for all applications that are used by the District to gather, store, and process data.
- There are still cloud-based applications containing sensitive data that do not have multi-factor authentication.
- The Office of Technology did not have a vulnerability scan performed in fiscal year 2018, however one was performed in fiscal year 2019 (March). As part of vulnerability management, IT management should also perform regular vulnerability scanning & remediation.

Audit Issues by Risk Level

High: 22 | **Moderate**: 36 | **Low**: 15

(7 Open) (27 Open) (7 Open)

Executive Summary

Background

This Follow-up Report presents the current status of the Management's Corrective Action Plans that were developed in response to the recommendations contained in the initial Information Technology (IT) Audit Reports. Schneider Downs & Co., were engaged to complete these audits.

The initial reports were approved for the release by the Audit and Accountability Committee on June 17, 2014, October 27, 2016, and August 17, 2017. The initial reports contained seventy-three (73) recommendations and related management corrective action plans.

There have been two IT Follow-up reviews approved for release by the Audit and Accountability Committee on March 26, 2015 and August 17, 2017.

For this Follow-up Review, we tested the outstanding high-risk recommendations (**2014** - #2, #8, #11) (**2016** - #1, #2) (**2017** - #2, #10, #11) that were still outstanding.

Roles and Responsibilities

District management is responsible for follow-up and corrective action to address audit recommendations. To fulfill this responsibility, the Office of Internal Audit has a process in place to track the status of corrective action plans and ensure that audit issues are adequately resolved.

Objective

The objective of this follow-up review is to ensure that management has taken corrective action to address the control deficiencies identified by the Office of Internal Audit.

Scope

The IT Audit follow-up work was completed in Fiscal Year 2019 and included a review of information from the period of July 1, 2018 through May 3, 2019.

Approach and Methodology

To complete this follow-up audit we performed the following procedures:

- Reviewed the prior Information Technology audit reports and the corrective action plans that were approved by the Audit and Accountability Committee;
- Interviewed IT staff and other relevant District staff to gain an understanding of the corrective actions taken and determine the status of the corrective actions according to management;
- Analyzed available information to validate information obtained during staff interviews; and

- Tested available documentation to determine if corrective actions have been fully implemented, are operating as management intended, and addressed all issues included in the above referenced audit report.

Results

We consider an issue resolved if management implemented their corrective action plan or took other appropriate action to resolve the identified issues.

The Office of Internal Audit found that management took sufficient corrective action for recommendations (2014 - #8, #11), resulting in 25% (2 of 8) of the tested issues from the IT Audit Reports. OIA concluded six (6) recommendations (2014 - #2) (2016 - #1, #2) (2017 - #2, #10, #11) were not implemented. Overall, management took sufficient corrective action for 44% (32 of 73) of the recommendations. This audit report was reviewed with management and they agreed with the conclusions.

Audit Year	Implemented	Not Implemented
2014	#8, #11	#2
2016	Not Applicable	#1, #2
2017	Not Applicable	#2, #10, #11

The Office of Internal Audit classified each issue into one of the following categories based on the work that we performed regarding the corrective action plan prepared by management and approved by the Audit and Accountability Committee:

Implemented – Action described in the corrective action plan prepared by management has been fully implemented and testing performed by Office of Internal Audit staff validated that the actions are working as management intends.

Not Implemented – There was insufficient evidence that the corrective action plan prepared by management was fully implemented.

Management Accepted the Risk – Risk concerning this issue was accepted by management and therefore no corrective action was taken.

Alternate Means – There was a significant change to the internal control environment regarding this recommendation and compensating controls and/or other methods were used to satisfy the recommendation.

Not Tested – The corrective action plan was not ready to be tested by the Office of Internal Audit or it could be tested more efficiently during another time.

SUMMARY OF RECOMMENDATIONS – FOLLOW-UP

Based upon the procedures performed, a number of issues having high degrees of risk were noted. The following table outlines the recommendations, the risk ratings assigned to each and the follow-up status. The definition of each rating's significance is noted below the table.

Recommendations	Risk Rating			Follow-up Status
	1	2	3	
2014 – IT Audit Report				
Recommendation No. 2 – (Logical Access - Weak Password Settings or No Password Requirements) The password policy standard needs to be created by management. Upon completion of the password policy, management should determine if the RighTrak and VersaTrans can meet the new password requirements. If application limitations exist, management should document the limitations as an exception to the policy.	X			**Not Implemented**
Recommendation No. 8 – (Job Scheduling - No Policy or Procedures) Management should develop a policy and procedures surrounding job scheduling. The policy should include how changes are to be requested, approved and documented. Until the job scheduling accounts are assigned with individual user access, a list should be maintained and documentation kept supporting these changes. A periodic review should be implemented to review that changes are authorized.	X			**Implemented**
Recommendation No. 11 – (Network - Windows XP Machine Still Active) OIA recommended the IT Department retire / replace existing Windows XP machines prior to April 8, 2014.	X			**Implemented**
2016 – IT Audit Report				
Recommendation No. 1 – (Internal IT Risk Assessment is Not Performed) The Information Technology Department should perform an	X			**Not Implemented**

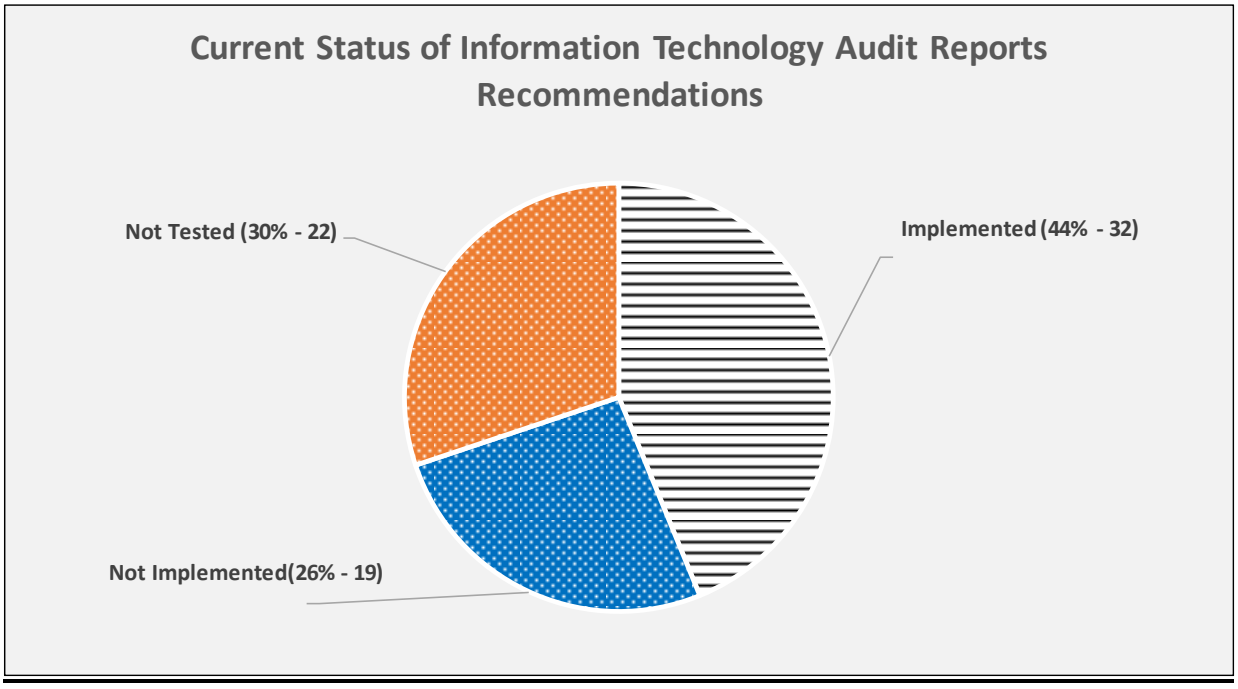
Recommendations	Risk Rating			Follow-up Status
	1	2	3	
annual self-assessment of risk and use the results for planning and establishment of risk tolerances within specific areas. Per COBIT best practice, the CCS administration should evaluate the results of the IT risk assessment and approve proposed IT risk tolerance thresholds against the enterprise's acceptable risk and opportunity levels.				
Recommendation No. 2 – (Formal IT Governance Structures Are Not in Place) We recommend that an approach to IT governance be adopted by CCS that weighs the benefits and goals of these activities against district objectives and constraints (e.g., costs, resources). At a minimum, CCS should establish an IT Steering Committee to ensure that effective communication is occurring across all lines of business.	X			**Not Implemented**
2017 IT Audit Report				
Recommendation No. 2 – (Logical Access - Enterprise Application User Access Reviews Not In Place) Implement an enterprise-wide, comprehensive user access review process for all applications that are used by the District to gather, store, and process data. This includes a process for identifying applications used by departments as well as application owners that are responsible for ensuring that only authorized users have access to district resources and data.	X			**Not Implemented**
Recommendation No. 10 – (Data Security - Ongoing Vulnerability Management Program Not In Place) There are affordable vulnerability management tools that scan the network on a daily basis and notify security personnel of new vulnerabilities. It is recommended one of these tools be acquired and leveraged as part of a vulnerability management program. Critical/high vulnerabilities should be remediated immediately; other vulnerabilities should be classified and managed accordingly based on the perceived threat level.	X			**Not Implemented**

Recommendations	Risk Rating			Follow-up Status
	1	2	3	
Recommendation No. 11 – (Data Security - Lack of Multi-Factor Authentication to Cloud-Based Applications) For all cloud-based applications containing sensitive data, enable multi-factor authentication. If the vendor does not support multi-factor authentication, request that this feature be added or evaluate alternatives.	X			**Not Implemented**

Risk Ratings

1 - High: Unacceptable risk requiring immediate corrective action;
2 – Moderate: Undesirable risk requiring future corrective action; and
3 – Low: Minor risks that management should assess for potential corrective action.

Summary Charts



Open issues by risk level

Risk level		High	Moderate	Low
Total recommendations		22	36	15
Implemented		16	9	8
Not Implemented		6	11	2
Not Tested		1	16	5
Open issues		7	27	7

Information Technology Audit Reports, Recommendations, Corrective Action Responses, OIA Work Performed, and Current Status for those issues that were not deemed to be successfully implemented as a result of our testing.

2014 High Risk Rating Issues (Comments)

Recommendation No. 2 – (Logical Access - Weak Password Settings or No Password Requirements)

The password policy standard needs to be created by management. Upon completion of the password policy, management should determine if the RighTrak and VersaTrans can meet the new password requirements. If application limitations exist, management should document the limitations as an exception to the policy.

Management Response

Both of these systems are locally managed in the Food Services and Transportation departments. IT has been in contact with both of the application owners and will be working with them and the vendors to establish procedures that will mirror the procedures in place for all CCS applications.

OIA Work Performed:

As noted in the Information Technology Audit dated August 2017, RighTrak and VersaTrans cannot comply with procedure due to application limitations.

Based on inquiry with the Director of the Office of Food Services and the Executive Director of the Office of Transportation no established procedures were performed to mirror the procedures in place for all CCS applications.

Further inquiry with the Director of the Office of Food Services, his office is in the process of issuing a Request for Proposal (RFP) for a new point of sale system. One of the system requirements of the RFP is that any new system would meet all CCS password requirements. The Office of Food Services expects to have a new system installed during fiscal year 2020.

Further inquiry with the Office of Transportation management there was a forced password reset of all users during the summer of 2018. OIA contacted Tyler's VersaTrans and was able to obtain instructions on how to do a forced password change every 90 days.

Update August 2019: The Office of Transportation did a forced password change for all users in July 2019. OIA was able to verify that the configuration occurred for a forced password in July 2019, however users will not be required to reset passwords until 90 days after their first login occurring in July or after. OIA will follow-up in late fall or winter to confirm user password changes.

Current Status: Not Implemented

New Implementation Date: FY20 (Food Service – New point of sale system) and July 2019 (Office of Transportation)

Process Owner(s): Director of the Office of Food Services and the Executive Director of the Office of Transportation

2016 High Risk Rating Issues (Comments)

Recommendation No. 1 – (Internal IT Risk Assessment is Not Performed)

The Information Technology Department should perform an annual self-assessment of risk and use the results for planning and establishment of risk tolerances within specific areas. Per COBIT best practice, the CCS administration should evaluate the results of the IT risk assessment and approve proposed IT risk tolerance thresholds against the enterprise's acceptable risk and opportunity levels.

Management Response

Initial Management Response October 27, 2016: Schneider Downs provided a document on what they would be looking for as a follow up. Both of the documents, manual and the risk template require significant work on the part of the IT department. IT will work through this plan, with the assistance of the Office of Internal Audit, to develop a strong risk assessment tool.

Target Implementation Date: *6/30/17*

Management response on 8/17/17, Schneider Downs, provided a document on what they would be looking for as a follow up. Both of the documents, manual (107 pages) and the risk template (112 lines) require significant work on the part of the IT department. This work is important and the assumption is after the process is worked through the first time, it will be a matter of updating the assessment annually.

While IT recognizes the need for all these, the current staff size of the department does not allow for the creation and management of a comprehensive plan in both of these areas. It is in our future staff development plan to hire a staff member to manage IT security and the DR Plan/COOP plans. Again, we are hoping for allocation for at least one staff member to manage these pieces and it is something we will build on annually. This will still be a significant undertaking for only one staff member.

OIA Work Performed:

Based on inquiry with IT Director on January 28, 2019, this is a goal for this year 2018-19, but operational needs have taken all of the director's time to date.

Update August 2019: This is something that we look forward to implementing when we have a CIO.

New Implementation Date: TBD

Current Status: Not Implemented

Recommendation No. 2 – (Formal IT Governance Structures Are Not in Place)

We recommend that an approach to IT governance be adopted by CCS that weighs the benefits and goals of these activities against district objectives and constraints (e.g., costs, resources). At a minimum, CCS should establish an IT Steering Committee to ensure that effective communication is occurring across all lines of business.

Management Response

Initial Management Response October 27, 2016: *Short-Term Plan:*

1. *Establish an IT Steering Committee with principals, teachers and IT operations staff. In addition, students will be included when we can bring them in, as they are the largest customer base. When necessary members of the operational/business areas of CCS will be engaged. The plan is for the meetings to occur monthly, beginning in September through the end of the school year. There may be occasions where more frequent meetings will need to occur or meetings may need to be cancelled based on the school calendar. All committee activity will be reported to the Senior Executive Director of Business and Operations.*
2. *The IT department is currently reporting weekly statistical information to the Senior Executive Director of Business and Operations regarding help desk and field team performance. In addition, the IT department collects real time data on the network performance. Moving forward, the business and operations group is evaluating software programs that allow for real time collection and reporting of performance metrics. IT will participate fully in this endeavor. This tool will allow for analysis of the data, and will provide reporting for the steering committee to make recommendations on IT and*

organizational changes that will better meet the needs of the customers.

Initial Management Response October 27, 2016: While IT recognizes the need for all these, the current staff size of the department does not allow for the creation and management of a comprehensive plan in both of these areas. It is in our future staff development plan to hire a staff member to manage IT security and the DR Plan/COOP plans. Again, we are hoping for allocation for at least one staff member to manage these pieces and it is something we will build on annually. This will still be a significant undertaking for only one staff member.

OIA Work Performed:

Based on inquiry with IT Director on January 28, 2019, this is a goal for this year 2018-19, but operational needs have taken all of the director's time to date.

Update August 2019: This is something that we look forward to implementing when we have a CIO.

New Implementation Date: TBD

Current Status: Not Implemented

2017 High Risk Rating Issues (Comments)

Recommendation No. 2 – (Logical Access - Enterprise Application User Access Reviews Not In Place)

Implement an enterprise-wide, comprehensive user access review process for all applications that are used by the District to gather, store, and process data. This includes a process for identifying applications used by departments as well as application owners that are responsible for ensuring that only authorized users have access to district resources and data.

Management Response

This finding will be divided into parts, beginning with a survey of the Chief Officers to collect a list of district applications, the associated application owner and the details on how users are assigned and managed for each of the applications reported.

IT will then work with the business owners to set up a process for reporting that each application has been reviewed annually to ensure the users assigned and their access are appropriate.

The Schneider Downs audit group did indicate that this type of access review would normally be managed by a risk team, outside of the IT department.

Implementation Date: Work will begin on this immediately following acceptance of the plan and will be a continuous district effort, 8/17/17.

OIA Work Performed:

OIA requested the survey emails sent to Chief Officers to collect a list of district applications and the associated application owners, details on how users are assigned and managed for each of the applications reported, and documentation that each application has been reviewed annually.

OIA did not receive any of the requested items above during our review.

Update August 2019: This is in progress as we move through the COOP planning process. It is helping IT to identify all of the applications used as many are web based. This is also assisting IT with ensuring we have the correct priority on applications for DR Planning and ensuring we have data sharing agreements for all applications that use the District's student and staff PII.

New Implementation Date: TBD

Current Status: Not Implemented

Recommendation No. 10 – (Data Security - Ongoing Vulnerability Management Program Not In Place)

There are affordable vulnerability management tools that scan the network on a daily basis and notify security personnel of new vulnerabilities. It is recommended one of these tools be acquired and leveraged as part of a vulnerability management program. Critical/high vulnerabilities should be remediated immediately; other vulnerabilities should be classified and managed accordingly based on the perceived threat level.

Original Management Response

After a more in depth discussion with Schneider Downs regarding this finding. It is our understanding that there are reasonably priced vulnerability scans that can be purchased and run at regular intervals. The IT department will investigate this as a strategy and purchase in FY18 if the budget will allow. In addition, the IT department will have a penetration test conducted annually. The penetration test was approved in the FY18 budget. ***Target*** **Implementation Date:** *Fiscal Year 2018*

OIA Work Performed:

Based on inquiry with the Director of Technology, the Office of Technology did not have a penetration test conducted in fiscal year 2018. For fiscal year 2019, the Director of Technology indicated, the Office of Technology contracted with a vendor to do penetration test and vulnerability scan.

As part of vulnerability management, IT management should also:

- Perform regular vulnerability scanning & remediation;
- Security training / phishing; and
- Security patch management.

Current Status: Not Implemented

Original Recommendation No. 11 – (Data Security - Lack of Multi-Factor Authentication to Cloud-Based Applications)

For all cloud-based applications containing sensitive data, enable multi-factor authentication. If the vendor does not support multi-factor authentication, request that this feature be added or evaluate alternatives.

Original Management Response

The IT department has already begun implementing this on systems we own and it is feasible. Additionally, we will review this recommendation with the individual application state holders to assess need, vendor capabilities, and risks associated with this finding to determine next steps.

***Target* Implementation Date:** *TBD*

OIA Work Performed:

Based on inquiry with the Director of Technology, on February 12, 2019 the Office of Technology implemented a security question verification to Tyler Technologies – Employee Self Service (ESS) login.

Currently, there are still cloud-based applications containing sensitive data that do not have multi-factor authentication.

Update August 2019: This is currently on all accounts with administrative rights to the data and backend servers and the network devices.

New Implementation Date: TBD

Current Status: Not Implemented