2017 Information Technology Audit

August 17, 2017

August 17, 2017

Dear Audit and Accountability Committee:

On behalf of Schneider Downs, we thank you for our continued partnership in assisting the Internal Audit Department in the performance of the Information Technology Audit for Columbus City Schools. The scope of the 2017 audit is outlined in this report. Our report includes the following sections: Executive Summary, Background, Scope and Objectives, and Summary of Observations. In addition to this report, a separate risk assessment has been provided detailing our observations from the risk assessment that was performed prior to this engagement. This was the first year that a comprehensive information technology risk assessment was performed; the risk assessment results should be used to drive future audit scope.

It should be recognized that controls are designed to provide reasonable, but not absolute assurance that errors and irregularities will be prevented, and that procedures are performed in accordance with management's intentions. There are inherent limitations that should be recognized in considering the potential effectiveness of any system of controls. Furthermore, the projection of any evaluation of controls to future periods is subject to the risk that the controls may become inadequate due to changing conditions and that the degree of compliance with procedures may deteriorate. Additionally, though a review of evidential matter and other procedures performed may suggest specific controls are functioning effectively, there remains the risk that controls may not have been functioning effectively or consistently throughout the prior periods.

The accompanying internal audit report is the result of our internal audit conducted in accordance with the Statements on Standards for Consulting Services of the American Institute of Certified Public Accountants. In accordance with our engagement letter, this internal audit did not constitute an audit of financial statements in accordance with generally accepted auditing standards. This report has been prepared for use by Internal Audit, Audit and Accountability Committee, and the Information Technology Management of Columbus City Schools.

Please contact me (614-586-7257/dowens@schneiderdowns.com) or Chris Debo (614-586-7108/ cdebo@schneiderdowns.com) if you have any questions.

Sincerely,

Donald R. Owens
Shareholder, Risk Advisory Services

cc: Dr. J. Daniel Good, *Superintendent*
Mary Jo Hudson, *Audit & Accountability Committee Chair*
Carolyn Smith, *Internal Auditor*
Michele VanDyke, *Director of Information Technology*

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report summarizes the findings from the Columbus City Schools 2017 information technology audit performed by Schneider Downs on behalf of the Internal Audit Department. The background, scope, objectives and findings are detailed in subsequent sections, as are follow-up audits of 2016 and 2014 audit findings that had yet to be remediated and validated. A risk assessment was also performed in 2017; this has been provided in a separate report, although the results of the risk assessment were incorporated into the 2017 audit approach.

There were 34 observations in 2017, split evenly between the Office 365 security audit and the other audit areas (logical access, data security, and data governance). Most of the Office 365 findings were identified via automated scans of system configuration settings, and many have already been remediated, while other require additional assessment to determine the cost associated with implementation.

The 17 observations not associated with Office 365 were also evenly divided within their respective audit areas, with 7 logical access observations, 5 data security observations, and 5 data governance observations. These observations had many shared underlying risks and recommendations, and could be classified as follows:

- **Shared and Unused Accounts** - There are numerous shared and/or generic Active Directory accounts, as well as many that have not been accessed in several years. Effective account management should minimize the number of accounts on a system (to minimize risks) and should ensure accountability and traceability of activity. Shared accounts limit this accountability.
- **Ethernet Port Accessibility and Lack of Network Segmentation** - Many Ethernet ports in district buildings are active and accessible. Because there is not any network segmentation, this increases the risk of unauthorized access to networked systems by malicious threat actors.
- **Lack of Multi-Factor Authentication for Web-Based Applications** - Several web-based applications (most notably Infinite Campus) do not require multi-factor authentication. If a user's credentials were obtained (due to theft or negligence) the threat actor would have access to all of the Infinite Campus modules and data to which the user has been provisioned access.
- **Decentralization of Core Data Governance, Logical Access and Change Management Functions** - Many essential information technology functions have been defined and implemented independent of a central authority, making coordination, consistency and oversight difficult (if not impossible).

Another observation that still persists from prior-year audits is that there are still several networked Windows XP machines. Given the other information security observations, these pose a significant threat to the security of the district's systems and data. The Information Technology Department is currently evaluating options to replace these systems; however, it is recommended that they be removed from the network immediately.

Another prior-year observation of note that has yet to be remediated is the inability to obtain and evaluate Security Organization Control (SOC) reports for vendor's that provide the district's core technology (Infinite Campus and MUNIS). These keeps the district in the dark in regards to significant risks associated with these technologies that the Information Technology Department should be aware of.

Lastly, in addition to these observations, a consistent resource management theme that is still open from the 2014 audit is that there is still no information technology representation on the Senior Leadership Team, and the Information Technology Department as a whole does not have sufficient staffing to achieve the security objectives that should be expected of an organization of the district's size. Mitigating the risks identified in this report and the risk assessment requires considerable investment; the district as a whole needs to determine its appetite for risk and allocate resources to achieve the desired level of safety.

BACKGROUND, SCOPE AND OBJECTIVES

Following up on prior year information technology audits, Columbus City Schools (CCS) requested Schneider Downs & Co., Inc. (Schneider Downs) to assist in developing and executing a comprehensive multi-year IT internal audit program and risk assessment that captures key processes, procedures and controls residing in both information technology operations and within the CCS user community.

The 2017 audit focused on enterprise logical access controls, data governance, data integrity, data security, and Office 365 security (refer to following sections for specific scope and objectives). In addition, Schneider Downs followed up on prior-year observations to determine if agreed upon controls have been implemented and are operating effectively.

Although a risk assessment was also performed as part of this engagement, the scope of the audit itself had already been established prior to the risk assessment. Therefore, specific areas of risk identified during the risk assessment were not incorporated into the 2017 audit plan (unless already related to the existing 2017 scope). This report includes observations from the audit; risk assessment results have been provided in a separate report.

Going forward, future audits will continue to assess the design and operating effectiveness of ITGCs, while also incorporating the results of the risk assessment from the prior year. As such, the confirmed approach for the 2018 will include the following:

- **Enterprise IT Risk Assessment Refresh** - Update the 2017 IT risk assessment to reflect the current IT environment.
- **Enterprise Technology Optimization Review -** Analysis of CCS' use of technology to enable and achieve district objectives. A full inventory of district software and partners will be performed, including a breakdown of purpose, use, and value derived from each. Recommendations will be made for enhancing the district's application portfolio through cost management, consolidation and optimization.
- **ITGC Audit (All Areas)** - Comprehensive review of IT general controls across the enterprise including change management, logical access, security, operations and job scheduling. The ITGC audit in 2018 will be comprehensive and enterprise-wide, expanding beyond the limited scope of applications reviewed in 2014 and the logical access review performed in 2017.
- **Other Areas Identified in 2017 Risk Assessment -** As with any risk assessment, it is expected that unanticipated areas of IT risk will be identified during the risk assessment. These will also be evaluated, prioritized and audited in 2018.
- **2017 Audit Observations Remediation Review** - Review of prior-year audit exceptions and status.

Prior-year information technology audits focused on typical IT general controls (ITGCs) and areas that were of specific concern due to historical problems and/or perceived risk. Given that the areas selected for the 2017 audit were determined prior to the risk assessment, a similar approach was taken. Based on observations from prior audits, areas of risk had been identified that had yet to be audited. These areas formed the basis for the 2017 information technology audit, and are broken down as follows:

IT General Controls - Logical Access

Prior-year logical access audits focused on core CCS applications. The 2017 audit included a comprehensive review of logical access across all departments and associated applications (a full list can be found in Appendix A). Logical access control design evaluation and testing included:

- User access and security procedures
- Administrative and privileged user access
- New and transferred employee access provisioning
- Terminated employee access removal
- User access reviews
- Password settings

Data Security

In addition to the logical access and Office 365 testing that was also performed, the data security audit focused on protection of student and staff data at rest. Given the limited number of hours that could be dedicated to this effort, focus was placed on the following areas identified as high-risk:

- Data security procedures
- Personnel security training
- Addressing vulnerabilities identified during the 2016 penetration test
- Physical security of data access points within the district

Also, an additional vulnerability assessment was performed on CCS' internal network based on the level of access available to anyone with access to an enabled Ethernet port. In total, 182 internal hosts were identified and scanned. A summary of observations is found in this report; the complete details were provided to the Information Technology and Internal Audit Departments.

Data Quality, Governance and Integrity

Given the volume of data collected, transformed and reported by CCS, data quality and governance are crucial to district operations and compliance. Although this audit evaluated data quality and governance across the district, the primary area of focus was the Department of Accountability and Other Support Services. This department is responsible for enterprise collection, analysis and reporting of data, including internal management reporting, state and federal reporting, and creation of internal and external reporting applications including CCSDAS and CCSD².

The focus of the audit was to identify and assess structures, procedures that govern data management and have the potential to cause data quality issues that could impact district reporting and operations. Audit procedures included:

- Reviewing existing data management procedures
- Reviewing change management procedures for reporting applications
- Assessing processes for ensuring data integrity across the enterprise
- Evaluation of EMIS reporting procedures and controls
- Testing change management for internal and external data requests
- Testing published reports and dashboards for data quality issues
- Testing of the data quality check application (Certify) processes and management

Office 365 Security

Office 365 has many built-in controls for optimization, preventing data theft/loss and accidental e-mailing of confidential information, scanning/filtering of inbound e-mails, and other security controls. The focus of this audit was on the configuration of Office 365 and associated processes for securing CCS data stored and processed in Microsoft's cloud. Specific audit steps included:

- Automated scan of the Office 365 environment to identify configuration settings that do not align with Microsoft's recommended settings
- Evaluation of automated scan observations for false positives
- Identification and testing of manual controls in place for securing Office 365 data

The Office 365 audit had significantly more observations than the other audit areas. This is primarily due to the fact that Microsoft provides an automated tool for scanning the entire Office 365 environment for configuration vulnerabilities; such functionality does not exist in other areas. This does not mean that Office 365 is the most vulnerable of the areas audited, it is merely a result of the availability of the tool that automates testing and allows for a more in-depth assessment than is attainable in manual audit areas.

The observations included in this report are the result of careful review and analysis, both of the observations themselves and the intent of the configuration settings desired by CCS. Only those observations that were determined to be non-optimal have been included; the complete Office 365 report has been provided to the Information Technology and Internal Audit Departments.

Prior-Year Audit Observations Remediation Review

This was a review of prior-year audit exceptions and status (both 2014 and 2016 audits). Our evaluation determined 1) if the observation has been addressed and 2) if the implemented control(s) are operating effectively.

Note: In management responses to prior year observations it was noted that some observations would not be remediated prior to the 2017 audit. These were excluded from testing and will be evaluated in 2018.

2017 AUDIT OBSERVATIONS

Based upon the procedures performed, a number of recommendations having varying degrees of risk were noted. The following table outlines the risk ratings assigned to each issue, as well as the status of each observation. The definition of each rating's significance is as follows:

- High - Risk requiring immediate corrective action
- Medium - Risk requiring future corrective action
- Low - Risks that management should assess for potential corrective action

Management was given the option to respond to the observations as follows:

- Agree with the observation and remediate ("Remediate")
- Agree with the observation and manage via existing vulnerability program ("Manage")
- Agree with the observation and accept the risk ("Accept")
- Agree with the observation but identify mitigating factors ("Mitigated")
- Disagree with observation ("Disagree")

Observation	Risk Level	Response
Logical Access		
1. Active Directory Passwords Set to Never Expire	High	Remediate
2. Enterprise Application User Access Reviews Not In Place	High	Remediate
3. MUNIS and VersaTrans Access Review Not Performed	Moderate	Remediate
4. Ineffective User Access Deprovisioning	Moderate	Remediate
5. Minimum Password Standards Not Enforced	Moderate	Remediate
6. Stale Infinite Campus Account Access	Moderate	Remediate
7. Shared Vendor Accounts	Moderate	Accept
Data Security		
8. Insufficient Physical Network Access Security	High	Accept
9. Port-Level Security Not Enforced	High	Accept
10. Ongoing Vulnerability Management Program Not in Place	High	Remediate
11. Lack of Multi-Factor Authentication to Cloud-Based Applications	High	Remediate
12. No Employee Security Awareness Training	Moderate	Remediate
Data Quality, Governance and Integrity		
13. Inadequate Testing of Production Reports and Dashboards	High	Remediate
14. Lack of Formal Data Classification Procedure	Moderate	Accept
15. Lack of Documented Data Governance Procedure and Structures	Moderate	Remediate
16. Lack of Enterprise Data and Reporting Change Management Procedures	Moderate	Remediate
17. Lack of Evidence of Data Request Testing	Moderate	Remediate
Office 365		
18. Data Loss Prevention Not Enabled	High	Remediate
19. Multi-Factor Authentication (MFA) Not Enabled	High	Remediate
20. Shared Office 365 Global Administrator Account	High	Remediate
21. Weak Mobile Device Password Setting	Moderate	Remediate
22. Unrestricted Access to Administrator Account Password	Moderate	Remediate
23. Intune Mobile Device Management Not Being Used For Mobile Device Access	Moderate	Remediate

24. Advanced Security Management Console Procedures Have Not Been Adopted	Moderate	Remediate
25. Advanced Threat Protection Safe Links/Attachments Procedures Have Not Been Adopted	Moderate	Remediate
26. Majority of User Accounts Do Not Have Mailbox Auditing Enabled	Moderate	Remediate
27. Mobile Device Encryption Not Enforced	Moderate	Remediate
28. Lack of Comprehensive Data Loss Prevention Governance	Moderate	Accept
29. Activity Reports Not Monitored/Reviewed	Moderate	Remediate
30. No SharePoint Portal Expiration	Low	Remediate
31. Information Rights Management Protection Not Enabled	Low	Remediate
32. Anonymous Access Link Expiration Not Enabled	Low	Remediate
33. Jailbroken Mobile Devices Permitted	Low	Remediate
34. No Timeout of Outlook Web Sessions	Low	Remediate

The sections below contain the observations from the audit. Each observation includes the observation identified during the audit, associated risk, a recommendation to enhance the control environment and management response to resolve the observation.

Logical Access

Observation 1 - Active Directory Passwords Set to Never Expire (High Risk)

Passwords to a total of 1,381 enabled employee and contractor accounts as well as generic system accounts in active directory (AD) are set to never expire and are not in compliance with the AD password procedure that enforces a 90-day expiration. These exceptions along with details about and approvals of their procedure exemptions were not documented.

Risk:

Password expiration controls are an effective component of breach prevention and detection. If a threat actor were to gain unauthorized access to an account that access would persist indefinitely.

Recommendation:

Set all AD account passwords to expire after 90 days. Establish AD procedures so that all new accounts are set to expire in the same manner upon account creation.

Management Response:

The accounts identified in this finding are used for two reasons:

1. Special programs in the district. The most recent examples of this are generic logins created for summer school students that are out of district and the SAT testing. In both cases generic accounts are used for a specified period of time. They are not set to expire as they are disabled following the program.
2. AD accounts are assigned to equipment and are manually changed when necessary.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: Currently implemented. CCS IT expires all AD passwords for full time staff and students and a change is required every 90 days.
Internal Audit Response:

While some of these accounts are for special programs and equipment, there were individual users that were also included in the list provided to the Information Technology Department that do not have password expirations set. Additionally, while maintaining generic accounts without password expirations is convenient for managing of these accounts, they present additional risk, especially because they provide no level of accountability and traceability when used. Until these risks are addressed, this will be considered to be not remediated.

Observation 2 - Enterprise Application User Access Reviews Not In Place (High Risk)

Per inquiry with the respective application administrators, IA was informed that only the following three applications are currently included in some form of periodic user access review process: MUNIS, Infinite Campus, and VersaTrans. The number of existing active directory (AD) accounts is large and comprised of a total of nearly 65K user accounts assigned to students as well as employees in 100+ schools across the entire school district. IT management has not yet formally defined and implemented an user access review process to validate that privileged and general user access is appropriate in AD and several other key applications, such as those applications that store, receive or transmit sensitive student data.

Risk:

Unauthorized or stale access to systems increases the risk of unauthorized access to systems by internal threat actors, including disgruntled and terminated employees, as well as external threat actors through stolen credentials.

Recommendation:

Implement a 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 be normally be managed by a risk team, outside of the IT department.

Process Owner: Michele A. VanDyke, Director of IT and the individual application owners.

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

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 3 - VersaTrans Access Review Not Performed (Moderate Risk)

Per inquiry with the Director of Transportation, IA was informed that a quarterly review of the VersaTrans user accounts is performed. However, supporting documentation from the Q1 review was not able to be provided.

Risk:

Unauthorized access to VersaTrans could lead to confidential data disclosure.

Recommendation:

User access reviews for VersaTrans should be performed in accordance with established procedures and evidence of reviews (and corresponding remediation activity) should be retained.

Management Response:

The Versa Trans piece was being worked on with the Director of Transportation and the Operations Manager both of whom have since retired. That system is solely managed by the Transportation Department and the process owner should be changed. There is currently a search to fill each vacancy. I have forwarded the finding on to the person filling the position in the interim, so that it can be addressed by the new staff.

Process Owner: Director of Transportation

Implementation Date: TBD

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 4 - Ineffective User Access Deprovisioning (Moderate Risk)

The following observations were noted with regards to the effectiveness of the user access deprovisioning process in several applications:

- 2 of a sample of 30 terminated employees each have a corresponding CIMS application user account that is enabled and has not been deactivated for 147 days and 109 days, respectively, since their individual effective termination dates of 12/20/16 and 1/27/17.
- 1 account from a population of 36 VersaTrans user accounts, which was assigned to a former employee terminated on 8/23/16, was not deactivated until over 7 months after the employee's effective termination date.

NOTE: None of these aforementioned user accounts were assigned privileged access (e.g., administrator rights) or part of a formal (and documented) user access review process.

Risk:

Continued access to the network or applications after an employee termination poses a security threat, as these accounts could be compromised and used for malicious purposes.

Recommendation:

Application owners should review the aforementioned user accounts enabled in CIMS and VersaTrans and take the necessary actions for those accounts no longer required for business use. Additionally, IT management should develop, implement and enforce a formal user access review (UAR) process. The UAR should be performed periodically by IT/application owners to recertify the appropriateness of the access/permissions held by both privileged accounts and standard user accounts on the network and in key applications.

Management Response:

For the two software programs listed above, the process owners do not reside in the IT department. Once the list of applications/software and the process owners is determined, the IT department will work to put a structure in place to communicate the need for access reviews to the process owners.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: This work will be a continual process as we begin to identify all of the applications in the district that are managed outside of the IT department.

Internal Audit Response:

Internal Audit agrees with the remediation approach

Observation 5 - Minimum Password Standards Not Enforced (Moderate Risk)

Password controls are enforced in various applications that may not align with acceptable industry-standards to maintain reasonable protection and minimize risk of unauthorized access. Examples include the following: CIMS (password history = 5 and password complexity not enabled), VersaFit (failed attempts before lockout = 25) and VFA/FAMIS (min. length = 6).

Password controls are available in LobbyGuard and FasTrak (Food Service) but not configured to enforce a minimum standard of password strength and security in accordance with a corporate procedure.

Due to system limitations within the software, RighTrak (Food Service) and VersaTrans do not have the capability of enforcing robust password controls. For example, in the Routing and Planning software hosted by VersaTrans, there are no available password requirements with regard to strength and security. With the exception of enforced password changes upon initial log on to user accounts, other security requirements are limited and there are no available requirements regarding password strength for users of the VersaTrans software suite of TripTracker, OnScreen,and Elink.

Risk:

Lack of enforcement of strong passwords increases the risk of account compromise that can lead to unauthorized access to network and systems, or exposure or theft of sensitive data.

Recommendation:

IT management should develop and implement a district password procedure that dictates a minimum standard for password strength and security (i.e., expiration, lockout) for consistent enforcement across the network, applications, operating systems and databases.

Management Response:

IT does enforce a ninety day password change for Active Directory which syncs with two of our largest applications: Infinite Campus and Office 365. MUNIS requires a 90 day password change as well and the security for the password is set by Tyler, who owns the software.

Our district allows schools and departments to manage their own budgets and decentralized purchasing. Many applications are managed outside of IT and are purchased off the shelf or as a service. In those instances the district does not have the ability to control password management. When IT is involved in planning of a system, the vendor is always asked to enforce a 90 day password change.

Many applications and software purchases are web based in the district and do not require intervention of the IT department. Once the list of applications/software and the process owners is developed, the IT department will communicate the need for mandatory password changes to the application owners.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: This work will be a continual process as we begin to identify all of the applications in the district that are managed outside of the IT department.

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 6 - Stale Infinite Campus Account Access (Moderate Risk)

IA inspected the population of 6,063 enabled employee IC user accounts to determine the scope of inactive IC accounts (per evaluation of the "Date Last Accessed" column). Per testing of employee user accounts that had not been logged into, a total of 598 accounts were identified that had been inactive since a date between 4/10/13 and 12/31/16. IA traced each of the 598 IC accounts to the list of AD accounts and noted a corresponding AD account existed and was also enabled for each.

This was important with regards to access control as IC users must use their active directory (AD) account to access Infinite Campus, and must first successfully authenticate through active directory in order to use the AD account to gain access to the Infinite Campus system.

Risk:

Stale and enabled user accounts provide increased risk of unauthorized system access, in particular, if their passwords were to ever become comprised.

Recommendation

These IC accounts should be reviewed and disabled if they are no longer required.

Management Response:

(Task A): Many of these accounts are ones that IT added when Infinite Campus was first implemented and at that time Infinite Campus was not yet connected to Active Directory. CCS wasn't completely sure who might need access at the time. These accounts all start with an "E", followed by employee number. These accounts were mostly for bus drivers, custodians, etc. There are 2,196 of these accounts. While they are still active, users do not know about them, nor do they know what passwords would be. Furthermore, if they would happen to get in, they have no access to do anything, not even view student information. Per the recommendation, we will be deleting these accounts no later than September 30, 2017.

(Task B): Regarding other user accounts, there are some legitimate users who simply have not logged on in some time as revealed to you by making the phone call to the Executive Director whom you had selected. We will review the list provided and remove or disable accounts where appropriate by November 29, 2017.

Process Owner: Dr. Machelle Kline, Chief Accountability Officer

Implementation Date: Task A = by September 30, 2017 and Task B = November 29, 2017

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 7 - Shared Vendor Accounts (Moderate Risk)

Generic vendor AD accounts are allowed to be shared by multiple individuals for vendor support (maintenance and troubleshooting) purposes which prevents the tracking of each individual's system activities for accountability.

Risk:

Compromised contractor AD accounts could allow unauthorized access to network and other key resources, which could lead to disruption in business operations or the theft, exposure, or loss of sensitive data (e.g., student/employee information).

Recommendation:

Require that all AD accounts (both internal and external) be uniquely assigned by individual.

If unique accounts are not possible, implement a stricter password expiration policy for contractor accounts (e.g. 30 days).

Management Response:

For all individually assigned Active Directory accounts (students and staff), CCS adheres to a 90 day password change policy. All contractor accounts are managed in the same manner as CCS employee accounts.

The accounts identified in this finding are used for two reasons:

1. Special programs in the district. The most recent examples of this are generic logins were created for summer school students that are out of district and the SAT testing. In both cases generic accounts are used for a specified period of time. They are not set to expire as they are disabled following the program.
2. AD accounts are assigned to equipment and are manually changed when necessary.

Currently implemented. CCS IT enforces AD password expiration for all full time staff and students, as well as contract employees and a change is required every 90 days.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: NA

Internal Audit Response:

The remediation approach does not mitigate the risk of shared vendor accounts. Shared accounts should be minimized/eliminated as much as possible, and only used when there is a valid business reason that cannot be achieved without a shared account. These exceptions should be formally documented and accepted.

Data Security

Observation 8 - Insufficient Physical Network Access Security (High Risk)

During the course of the audit it was noted that the majority of Ethernet ports in CCS facilities are enabled and that the network is not segmented (all ports provide the same level of internal network access). While all facilities maintain some level of physical access security, many (especially administrative buildings that students do not attend) allow visitors to enter and access locations where Ethernet ports are available. A threat actor with malicious intent could pose as a visitor and connect to the internal network via this method.

Risk:

Unauthorized access within an internal network may lead to malicious activities such as identity theft, financial fraud, theft of sensitive data and even malicious attacks on systems (e.g., denial of service), if undetected.

Recommendation:

Physical ports should be disabled except in areas that are protected against unauthorized physical access.

Management Response:

Disabling physical ports and requiring everyone to use the wireless network is not feasible. All of our buildings do require secure physical access through key card or sign in at all buildings. In addition, the IT department has monitoring and detection tools in place.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: Complete

Internal Audit Response:

The identified risk has not been addressed or remediated. Exposed physical ports exist in most district buildings and can be accessed in some public spaces. In order to mitigate the risk, one or more of the following actions should be taken:

- Implementation of port-level security
- Disabling of physical ports that can be accessed in public or easily accessible spaces
- Implementation of network segmentation

Observation 9 - Port-Level Security Not Enforced (High Risk)

Physical Ethernet ports at CCS locations permit the discovery of CCS assets on the network by anyone physically connected to the network, even if they are using a device not issued by CCS. By connecting to an Ethernet port in the Kingswood Data Center, IA was able to discover 182 devices connected to the network. A subsequent vulnerabiilty scan identified a total of 49 critical/high vulnerabilities open to the immediate threat of compromise. The complete details of these have been provided to the Information Technology Department.

Risk:

Unauthorized access within an internal network may lead to malicious activities such as identity theft, financial fraud, theft of sensitive data and even malicious attacks on systems (e.g., denial of service), if undetected.

Recommendation:

Deploy necessary network security measures to restrict unregistered (i.e., district-issued) MAC addresses from connecting to the wired CCS networks. Guests should be guided to connect to a segmented guest wireless network.

Management Response:

Disabling physical ports and requiring everyone to use the wireless network is not feasible. All of our buildings do require secure physical access through key card or sign in at all buildings. In addition, guests are directed to the guest network. That network is intentionally set at a lower bandwidth and is segmented from the rest of the network. It is not designed to handle video and presentations that may require the district to allow guests onto the network.

This would require a build out of a second network for every building, that we do not have the staff to manage and it is cost prohibitive in relation to the overall risk.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: Complete

Internal Audit Response:

See Observation #8

Observation 10 - Ongoing Vulnerability Management Program Not in Place (High Risk)

An ongoing network vulnerability management program is not in place. A penetration test was performed in 2016, during which several critical vulnerabilities were identified. These were subsequently addressed; however, new vulnerabilities (such as the WannaCry vulnerability that resulted in the worldwide ransomware attack in May) are constantly being identified and leveraged by attackers. In April, IA performed a follow-up vulnerability scan on the 182 assets identified on the internal network and found 49 new critical/high vulnerabilities.

Risk:

Without an investment in an ongoing vulnerability management program (and required toolsets) the district will be vulnerable to attack.

Recommendation:

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.

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.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: FY18

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 11 - Lack of Multi-Factor Authentication to Cloud-Based Applications (High Risk)

Remote access to the hosted Infinite Campus application is only protected by single-factor authentication (user ID and password), unlike other key applications such as MUNIS, that require multifactor authentication to enable remote access.

Also, URL links available for CCS staff to log into key applications containing sensitive data, such as Infinite Campus, Employee Self Service and SEMS, are openly displayed on the landing page of the CCS portal (http://www.ccsoh.us/Staff), which is public-facing and accessible by any web browser.

Risk:

If a threat actor was able to obtain CCS employee credentials via a phishing attack or other means they would be able to access Infinite Campus through that user's account.

Recommendation:

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.

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.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: TBD

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 12 - No Employee Security Awareness Training (Moderate Risk)

There are no corporate-wide security awareness trainings available and required to be taken to help enhance employees' understanding of critical IT topics to the organization, such as the following:

- Security procedures
- Data classification and handling
- Desktop security
- Wireless networks and security
- Password security
- E-mail phishing scams, ransomware and malware

Risk:

Employees are the first line of defense in preventing cyber attacks. Security awareness training is a key component in preventing phishing attacks from being successful.

Recommendation:

Implement a security awareness program for all personnel and contractors. Require that, as part of being provisioned AD access, that this training be completed. The training should be refreshed annually and all employees and contractors should be required to participate on an annual basis.

Management Response:

There are very clear Board Policies regarding acceptable use of the district technology and the internet (7530.02 - 7543 and 8351). A course is also available in Public School Works "Cyber Security" that outlines measures employees can take to ensure the security of computer systems, respond to potential security violations, recognize essential and sensitive data and its associated protections, and identify authorized computer uses.

IT is working with CCS leadership to ensure that users are aware of the training opportunity.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: The Board policies are in effect and all employees were required to the acknowledge they have access and are familiar with the content through Public School Works, the course is currently available to all district employees.

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Data Quality, Governance and Integrity

Observation 13 - Inadequate Testing of Production Reports and Dashboards (High Risk)

IA identified several significant anomolies when evaluating the accuracy of published dashboards and reports (these are detailed in Appendix B). Such anomolies should be identified during testing. In many cases, it was determined (through inquiry) that reliance was placed on end-users for testing and approval of production reports.

Risk:

Placing reliance on end-users for report accuracy increases the risk of errors in production reports and analysis.

Recommendation:

The majority of report, analysis, and dashboard testing should be performed by unit testers and other personnel prior to providing to end users for user acceptance testing. Oftentimes in the case of data-related requests (reports, analysis, etc.) there is a tradeoff between deployment speed and accuracy. The district should prioritize accuracy and enact procedures that set a minimum standard of testing depending on the type of report, analysis, or dashboard being requested/developed.

Management Response:

The response below is specific to the CCSD2 dashboard for student information only.

Given the incredibly large amount of data on the dashboard, it is not feasible to identify, ahead of time, every possible anomaly that could occur.

End users did participate in testing, as their business knowledge was key to understanding what the final product should look like. Testing took place throughout development by both the application development team and by the business user support team. Further testing took place with additional end users prior to and after release as a monitoring agent.

Process Owner: Dr. Machelle Kline, Chief Accountability Officer

Implementation Date: Ongoing

Internal Audit Response:

This observation will be addressed primarily by the implementation of a district-wide change management standard (see Observation #16).

Observation 14 - Lack of Formal Data Classification Procedure (Moderate Risk)

A formal data classification procedure is not in place that classifies the types of data collected, processed and reported by the district and the required level of protection for each.

Risk:

Without a formal data classification scheme, it is difficult to implement programs to protect data across the enterprise. This can result in an increased risk of data loss.

Recommendation:

Build a formal data classification scheme that applies to the entire district. At a minimum, the definitions of data considered public, private, and confidential should be defined.

Management Response:

This observation has been noted. Currently, Ohio Revised Code does not require a formal data classification procedure. When and if this becomes necessary, we will work to complete this process.

Process Owner: Dr. Machelle Kline, Chief Accountability Officer

Implementation Date: N/A

Internal Audit Response:

Although not required by the Ohio Revised Code, CCS should consider adoption

Observation 15 - Lack of Documented Data Governance Procedure and Structures (Moderate Risk)

Although a large team has been organized under the Department of Accountability to meet the growing needs of data transparency and reporting within the district, formal data governance procedures and

structures are not in place to manage data quality and reporting. Examples of expected data governance documentation, based on best practice and industry standards, include:

- Assigned data owners and data stewards based on subject area
- Data steering committee team members, objectives, and meeting requirements
- Formal procedures for identifying, prioritizing, and responding to data quality issues
- Change management procedures for report/analysis/dashboard development, testing, approval, user acceptance, and deployment
- Procedures for data sharing, both internal and external
- Data dictionaries for core application data and data deployed through other mechanisms (e.g. the data warehouse, dashboards)

Risk:

Without formal data governance, the likelihood of data integrity and quality issues increases. This can result in inaccurate reporting, analysis, and publication of erroneous data to public sources and regulatory agencies.

Recommendation:

Leveraging documented industry best practices, formalize the data governance practice with CCS. While many best practices are already in place, many are ad-hoc or not formalized. In order to measure the success of data governance over time, these should be documented. Examples include procedures around the usage of Certify for managing data quality and requirements for communicating and remediating identified issues.

Management Response:

We have made great strides in improving our data accuracy and we recognize that there is always room to grow. With the implementation of Certify, we have started to provide end users a tool which empowers them to 'own' their data in a way they have not been able to before. We will continue to build on this successful platform throughout the 2017-2018 school year with more training, implementation of new rules, and improvement of existing rules.

During the 2017-2018 school year, we will examine the use of data governance in other K-12 school districts to determine if the recommended data governance is feasible and has a positive return on investment.

Process Owner: Dr. Machelle Kline, Chief Accountability Officer

Implementation Date: Examination of data governance by July of 2018

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 16 - Lack of Enterprise Data and Reporting Change Management Procedures (Moderate Risk)

Although change management procedures are in place for certain applications (Infinite Campus, for example), a formal change management process is not in place for all enterprise applications, including those associated with data acquisition, manipulation, reporting, and analysis.

Risk:

Without a consistent approach to development and analysis, the risk of data quality and integrity issues increase. This can result in erroneous data persisting throughout the enterprise as well as inaccurate reporting/analysis.

Recommendation:

Develop a formal change management process that applies to all enterprise information technology modifications, including (but not limited to) ETL development, DDL changes, report development, data request fulfillment, regulatory data submissions, data analysis, and dashboard development. Changes should include, at a minimum, a documented request for the change, version control, evidence of unit testing, approval for release, and end-user acceptance. The definition of a "change" should also be formalized within the district, as should the corresponding systems that are required to adhere to the process.

Management Response:

IT will develop a standard for all software upgrades and changes and communicate that to all staff. Software and web applications are not all managed in the IT department. This communication will give the owners guidelines for what to do in a situation where the software/application is going to be upgraded.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: FY18

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 17 - Lack of Evidence of Data Request Testing (Moderate Risk)

From a population of data requests provided by the Information Technology Department, IA requested evidence of report testing and approval for a sample of 25 requests. Evidence of testing could not be provided.

Risk:

If not adequately tested and approved, inaccurate reporting can result in poor management decision-making, loss of reputation, and financial penalties due to regulatory/compliance issues.

Recommendation:

Although a good program is in place for tracking of requests and (per inquiry) all requests are tested prior to release, evidence of testing and approval should be maintained for all data requests. The required level of testing for requests should be relative to the request complexity and percieved risk of reporting inaccuracy.

Management Response:

We have already implemented a peer review process. Within this update to the CCSDAS, we can now keep track of the review process electronically along with the initial data request, assignment of an analyst and approval/fulfillment. Although this process is now in place, we will continue to test and monitor this process throughout the 2017-2018 school year. The target date for complete implementation will be July of 2018.

Process Owner: Dr. Machelle Kline, Chief Accountability Officer

Implementation Date: Ongoing with complete implementation in July of 2018.

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Office 365

Observation 18 - Data Loss Prevention Not Enabled (High Risk)

IT has not adequately leveraged the built-in DLP capabilities provided by Office 365 by activating functions to automatically monitor outbound e-mail traffic and take necessary actions (e.g., alert, block) on detected PII.

Risk:

If applicable types of PII are not identified and protected accordingly, the district is at risk of leaving certain categories of PII exposed to breach.

Recommendation:

IT management should enable Data Loss Prevention (DLP) procedures to help protect data from accidental or malicious exposure.

Note: DLP allows Exchange Online and SharePoint Online content to be scanned for specific types of PII data (in conjunction with management directives and recommendations published in publication 800-122 by the National Institute of Standards and Technology) such as social security numbers, credit card numbers, and passwords, and will alert users and administrators that this data should not be exposed.

Management Response:

DLP is enabled for SSN.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: Complete

Observation 19 - Multi-Factor Authentication (MFA) Not Enabled (High Risk)

The Microsoft SecureScore Report found that all 10 CCS administrators did not have MFA enabled.

The Microsoft SecureScore Report also found that all 12,225 CCS users did not have MFA enabled.

Risk:

If an Office 365 administrator's account is compromised, the threat actor would have unlimited access to the Office 365 environment. A breach of any of those accounts can lead to a breach of CCS data.

Recommendation:

CCS should enable MFA for all of CCS accounts.

Management Response:

This feature will be enabled for administrator accounts.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: Complete

Observation 20 - Shared Office 365 Global Administrator Account (High Risk)

The password to an enabled user account named "Chris and Greg" holding global administrator privileges was shared between one current employee (Chris Francia) and another employee (Greg Sturgill) no longer employed with the company.

Risk:

If there is an security/data incident caused by a shared account, there is a risk of not being able to determine who caused the incident.

Recommendation:

IT management should decommission or delete the shared global administrator account called “Chris and Greg.”

Management Response:

The “Chris and Greg” account was decommissioned on 4/13/17.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: Complete

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 21 - Weak Mobile Device Password Setting (Moderate Risk)

A minimum password length of only 4 characters is enforced on mobile devices attempting to authenticate to the Office 365 platform.

Risk:

Lack of enforcement of strong passwords increases the risk of account compromise that can lead to unauthorized access to network and systems, or exposure or theft of sensitive data.

Recommendation:

IT management should enhance password requirements for mobile devices by enforcing a minimum password length of 8 characters in Office 365.

Management Response:

The district does enforce a password on mobile devices. For computers and laptops district authentication is required to get to Office 365. For phones and tablets, a 4 digit security code is required before district email will download.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: Complete

Internal Audit Response:

CCS should consider adoption of a 6-digit password standard for mobile devices.

Observation 22 - Unrestricted Access to Administrator Account Password (Moderate Risk)

Approximately 10 members of the IT department know the master password to the KeePass open-source password manager tool that centrally stores the passwords to the Global administrator system account in Office 365 as well as the administrator accounts for a number of other applications. As a result, each individual has access to all passwords stored in KeePass.

Limited features of this free tool do not include a granular-level of access control, as there is no functionality available to create and assign group-based, IP-based, or user-based permissions as a means to restrict individuals access to only the passwords commensurate with their job duties.

Risk:

Increased risk of someone inside the organization having the ability to access login credentials for critical accounts outside of their duties and elevate privileges that were not authorized.

Recommendation:

Have a master account that is only accessible by a few administrators and then create standard accounts for the remaining users/admins that need access to one or more of the passwords in the password manager. The designated administrators of the Master Account can then share specific passwords with users based on their job duties or through the creation of shared password folders that are accessible only to the users specified to have access to the folder.

Management Response:

Password is stored in KeePass. All CBTS server admins and a few others have access to KeePass.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: Complete

Internal Audit Response:

While KeePass is a useful tool for managing administrative passwords, the management response does not address the documented risk; administrators should only have access to passwords necessary to complete their job duties.

Observation 23 - Intune Mobile Device Management Not Being Used For Mobile Device Access (Moderate Risk)

The Microsoft SecureScore Report found that CCS enablement of mobile device management services is set to false.

Risk:

Mobile devices may have had basic protections disabled by unauthorized modifications, increasing the risk of a network breach or malware infection if connected to the network.

Recommendation:

CCS should use a mobile device management service such as Microsoft InTune. Devices, especially mobile devices, are vulnerable to attacks such as malware that can lead to account and data breaches.

Management Response:

This will be researched by the IT department to understand the impact to the end user community.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: TBD

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 24 - Advanced Security Management Console Procedures Have Not Been Adopted (Moderate Risk)

The Microsoft SecureScore Report found that CCS's subscription to Advanced Security Management Console is set to false.

Risk:

If the Advanced Security Management Console is not enabled, administrators may not be alerted of anomolous or suspicious Office 365 activity. This could result in a data breach going undetected.

Recommendation:

CCS should adopt the Office 365 Advanced Security Management Console. This console will allow CCS to set up procedures to alert administrators about anomalous and suspicious activity.

Management Response:

Advanced Security Management is available in Office 365 Enterprise E5 or as an add-on subscription to Office 365.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: This is an expense we will investigate as it is not part of the package offered to school districts.

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 25 - Advanced Threat Protection Safe Links/Attachments Procedures Have Not Been Adopted (Moderate Risk)

The Microsoft SecureScore Report found that CCS enablement of safe links/attachments protection is set to false.

Risk:

Without ATP enablement, the success of phishing attacks that leverage malicious links/attachments increases.

Recommendation:

CCS should enable the Office 365 Advanced Threat Protection Safe Attachments feature. This will extend malware protections in service to include routing all messages and attachments that don't have a known virus/malware signature to a special hypervisor environment where a behavior analysis is performed using a variety of machine learning and analysis techniques to detect malicious intent.

Management Response:

This has been enabled.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: Complete

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 26 - Majority of User Accounts Do Not Have Mailbox Auditing Enabled (Moderate Risk)

The Microsoft SecureScore Report found that only two CCS mailboxes have auditing enabled.

Risk:

In the event of an account's compromise, malicious activity may go undetected.

Recommendation:

CCS should enable mailbox auditing for all users that have mailboxes in the CCS Office 365 environment. By default, all non-owner access are audited, but CCS must enable auditing on the mailbox

for owner access to also be audited. This will allow CCS to discover illicit access of Exchange Online activity if a user's account has been breached.

Management Response:

This needs discussed as a team for end user adoption and impact.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: TBD

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 27 - Mobile Device Encryption Not Enforced (Moderate Risk)

The Microsoft SecureScore Report found the mobile device procedure does not enforce encryption on mobile devices (setting = false) connected to Office 365.

Risk:

Unencrypted mobile devices can be stolen and their sensitive data extracted by an unauthorized individual for malicious purposes.

Recommendation:

IT management should update the applicable mobile device procedure setting to true so mobile devices are required to encrypt all data accessible through their remote connections to Office 365 and other services.

Management Response: This feature has been enabled.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: Complete

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 28 - Lack of Comprehensive Data Loss Prevention Governance (Moderate Risk)

IA noted the following observations with regards to the existing Data Loss Prevention (DLP) functionality/process supported by Office 365:

- DLP functionality (or system procedure) is set to monitor attachments in outbound Outlook emails as well as shared documents from SharePoint and OneDrive and issue violation alerts for detected social security numbers (SSN). However, monitoring is limited in scope and notably excludes data such as credit card numbers, biometric data and other types of sensitive data.
- There is no formal process established where IT personnel periodically review and follow up on the violation alerts from the external e-mail transmissions that contained SSNs.
- The DLP system procedure has email-blocking and override capabilities available which are not enabled to prevent SSNs from leaving the district via e-mail without a documented business need.

Risk:

Improper configuration of Data Loss Prevention (DLP) technology could lead to unknown/unwanted transmission of sensitive data outside the internal network, exposing the company to the risk of a data breach. Without proper DLP protection, data leakage could occur through many channels, including company email, commercial email (e.g., Gmail), web browsers, or mobile devices (e.g., cell phones or flash drives).

Recommendation:

IT management should:

1. Expand the scope of monitored PII in accordance with a new corporate DLP procedure.
2. Enable e-mail blocking and override processes in Office 365.
3. Implement a periodic review process to evaluate all reported e-mail violations.

Management Response:

The IT department is currently monitoring for SSNs and does not look to expand the scope at this time.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: Complete

Internal Audit Response:

CCS should, as part of their risk management procedures, periodically evaluate the risks associated with data loss and determine if the scope of PII being monitored should be expanded.

Observation 29 - Activity Reports Not Monitored/Reviewed (Moderate Risk)

The Microsoft SecureScore Report found that several available Office 365 reports that are useful in preventing/detecting data breaches are not being accessed (and subsequently reviewed). These include:

- Global Administrator Role Change Report
- Sign-in Activity Report
- Audit Reports
- Malware Detection Reports
- Account Provisioning Activity Report
- E-mail Forwarding Rules Report
- Mailbox Access by Non-Owner Report
- Sign-ins After Multiple Failuers Report

Risk:

Attempted and/or successful data breach may go undetected. Illicit role group changes, which could give an attacker elevated privileges to perform more dangerous and impactful things in CCS Office 365 tenancy.

Recommendation:

CCS should review user role group changes at least every week. There are several ways CCS can do this, including simply reviewing the list of users in different administrative role groups in the Office 365 Admin Portal or by reviewing role administration activity from the Audit Log Search.

Management Response:

The district currently has one person managing Office 365 for the district. IT will begin to look at monitoring reports in 1 – 3 month intervals.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: This will begin once we have had to a chance to understand the volume and what the reports entail.

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 30 - No SharePoint Portal Expiration (Low Risk)

Authorized user access to SharePoint folders containing sensitive data is not set to expire after a specific amount of time.

Risk:

Employees may access SharePoint folders that they no longer need access to, which could result in unnecessary exposure or leakege of sensitive data.

Recommendation:

IT management should review access to the sensitive SharePoint folders on a periodic basis and remove any unnecessary/excessive access. Also, IT management should enable account expiration and configure the expiration according to a reasonable timeframe.

Management Response:

This will be set to one year.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: By January 2018

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 31 - Information Rights Management Protection Not Enabled (Low Risk)

The Microsoft SecureScore Report found that no CCS employees had IRM enabled.

Risk:

Without monitoring of document sharing, sensitive information could be intentionally or accidentally shared outside of CCS with unauthorized third-parties.

Recommendation:

CCS should enable and use Information Rights Management protections on email and document data. This will help prevent accidental or malicious exposure of CCS data outside of the organizational boundaries. Attackers targeting specific, high value data assets will be prevented from opening them without CCS credentials.

Management Response:

IT will further investigate this feature and how this information will be used.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: TBD

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 32 - Anonymous Access Link Expiration Not Enabled (Low Risk)

The Microsoft SecureScore Report found that the external link expiration time does not limit the length of time that anonymous access links are accessible (setting = False).

Risk:

Malicious links used by threat actors may persist in Office 365 indefinitely.

Recommendation:

CCS should restrict the length of time that anonymous access links are valid. An attacker can compromise a user account for a short period of time, send anonymous sharing links to an external account, then take their time accessing the data. They can also compromise external accounts and steal the anonymous sharing links sent to those external entities well after the data has been shared.

Management Response:

Anonymous access links are not allowed in the organization.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: Complete

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 33 - Jailbroken Mobile Devices Permitted (Low Risk)

The Microsoft SecureScore Report found that the mobile device procedure permits (setting = TRUE) jailbroken and rooted mobile devices to connect to the mail and other Office 365 services.

Risk:

Mobile devices connected that may have had basic protections disabled by unauthorized modifications, increase the risk of a network breach or malware infection due to their connections to the network and the activation of malicious software.

Recommendation:

IT management should update the applicable mobile device procedure setting to FALSE in order to prevent jailbroken and rooted mobile devices from connecting to Office 365.

Management Response:

This can be implemented after review of impact and set up procedures.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: TBD

Internal Audit Response:

Internal Audit agrees with the remediation approach.

Observation 34 - No Timeout of Outlook Web Sessions (Low Risk)

Outlook Web Access (OWA) sessions allow an inactive user to remain remotely connected to their Outlook email account from a public or shared computer for up to 6 hours without session timeout.

Risk:

Public workstations allowed to remain indefinitely logged into online services or unmanned for periods of time could allow the compromise of an account and lead to the theft, loss, or disclosure of sensitive data.

Recommendation:

IT management should update the session timeout configuration to enforce an inactivity timeout after 15 minutes (default value) from a public or shared computer.

Management Response:

Set to 6 hours.

Process Owner: Michele A. VanDyke, Director of IT

Implementation Date: Complete

Internal Audit Response:

Internal Audit agrees with the remediation approach.

2016 AUDIT OBSERVATION REMEDIATION STATUS

Of the 25 observations identified during the 2016 audit, 11 have been fully remediated as-of the 2017 audit and 2 have been Not Remediated. 12 remain open, as summarized below.

Observation	Risk Level	Management Action	Audit Observation
IT Governance			
1. Internal IT Risk Assessment Not Performed	High	Not Remediated	Not Remediated
2. Formal IT Governance Structures Not in Place	High	Not Remediated	Not Remediated
3. Balanced Scorecard Not in Place	Medium	Remediated	Remediated
4. Lack of IT Representative in Senior Leadership Team	Medium	Not Remediated	Not Remediated
Vendor Management			
5. PII Data Being Transferred to Third Parties via Unsecured FTP	High	Remediated	Remediated
6. No Security Guidelines or Minimum Control Requirements in Contracts	High	Remediated	Remediated
7. No Comprehensive Vendor Review Process	High	Remediated	Remediated
8. No Review of Vendor's Security Controls	Medium	Not Remediated	Not Remediated
9. No Regular Review of Vendor Contracts	Medium	Remediated	Remediated
10. Original Vendor Contract Not Available	Low	Remediated	Remediated
11. No Documented Legal Approval of Contract	Low	Remediated	Remediated
12. No Evidence of RFP or Solution Selection Process	Low	Remediated	Remediated
13. No Review of Shared Accounts on CCS-SFTP Site	Low	Not Remediated	Not Remediated
14. Talend Password(s) Used for FTP Jobs Hard-Coded in the Jobs	Low	Remediated	Remediated
IT Infrastructure			
15. User Acceptance Forms Not Required for Non-Fixed Assets	Medium	Not Remediated	Not Remediated
16. No Formal Tracking of IT Infrastructure Warranty Information	Low	Remediated	Remediated
17. IT Fixed Asset Updates Not Timely	Low	Remediated	Remediated
Disaster Recovery			
18. A Business Impact Analysis Has Not Been Performed	Medium	Not Remediated	Not Remediated
19. Application List in Disaster Recovery Plan Incomplete	Medium	Not Remediated	Not Remediated
20. Comprehensive Backup Testing Not Performed	Medium	Not Remediated	Not Remediated
21. No Data Redundancy Sites	Medium	Not Remediated	Not Remediated
22. SAN Still Being Utilized for File Storage Instead of Office 365	Low	Remediated	Remediated

Physical Security			
23. Access to the Kingswood Data Center Building Not Sufficiently Restricted	Medium	Not Remediated	Not Remediated
24. No Raised Floors at Hudson and Fort Hayes Data Centers	Medium	Not Remediated	Not Remediated
25. No Fire-Suppression Systems in Primary Data Centers	Medium	Remediated	Remediated

IT Governance

Observation 1 - Internal IT Risk Assessment Not Performed (High Risk)

Although an assessment of IT risk has been performed in the past by the Internal Audit Department, the Information Technology Department does not perform a formal assessment of risk within IT.

Recommendation:

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. In accordance with 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.

Initial Management Response:

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.

Management Action: Not Remediated

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.

Audit Observation: Not Remediated

Observation 2 - Formal IT Governance Structures Not in Place (High Risk)

A comprehensive IT governance structure is not in place at CCS. CCS's current governance consists of a monthly meeting between the Director of Information Technology and the Senior Executive Director of Business Operations. This meeting consists of general updates as well as a weekly technology report that covers the following:

- Field service statistics (e.g., open tickets)
- Service desk statistics (e.g., service desk queue)
- Outcomes/accomplishments for the month
- Emerging and ongoing issues

This report does not include a comprehensive and holistic view of IT operations and does not provide qualitative metrics for management of IT.
Recommendation:

Best practice for internal IT governance consists of the following:

1. Establishing an IT Steering Committee consisting of stakeholders within each of the schools and administrative departments.
2. Periodic (at least monthly) meetings to communicate changes within the schools/departments and identify challenges/opportunities within IT.
3. Establishment of formal short- and long-term IT maturity targets and implementation of a process for measuring and communicating progress towards these objectives.
4. Defining a balanced set of performance objectives, metrics, targets and benchmarks. These should be reviewed and agreed upon with both IT and business functions, and other relevant stakeholders.
5. Formalization of legal and regulatory IT risk and development of strategies to mitigate these risks.
6. Building a cybersecurity portfolio and creating processes for proactively monitoring cyber risk and reporting of events to leadership.
7. Alignment of application and infrastructure architecture to district objectives and risks.

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.

Initial Management Response:

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.

Management Action: Not Remediated

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.

Audit Observation: Not Remediated

Observation 3 - Balanced Scorecard Not in Place (Medium Risk)

CCS's current weekly status report (discussed in Finding 2) does not provide sufficient information for governance of IT. In addition to the status report, IT does provide annual metrics to the Council of the Great City Schools for aggregation and comparison. However, these metrics frequently change over time, are backwards-looking, and do not provide sufficient actionable information.

Recommendation:

CCS should create an executive dashboard that includes key measures for managing of IT. Similar to the recommendations for IT governance (Finding 2), this should contain the following:

1. Balanced set of performance objectives, metrics, targets and benchmarks. Metrics should cover activity and outcome measures, including lead and lag indicators for outcomes, as well as an appropriate balance of financial and non-financial measures.
2. Relevant, timely, complete, credible and accurate data to report on progress in delivering value against targets, including high-level views of portfolio, program and IT performance that supports decision making, and measures whether expected results are being achieved.

Metrics should be actionable and comparable. For example, instead of reporting on the open number of help desk tickets, a more valuable metric would be the relative increase/decrease in help desk tickets and response rates over the last month. Another example would be to track the expected vs. actual outcomes of implementing classroom learning technologies (i.e., students saw a 10% increase on state assessments).

A regular review (and least monthly) of CCS's progress towards identified goals and the extent to which planned objectives have been achieved, deliverables obtained, performance targets met and risk mitigated should be performed with the IT Steering Committee.

Initial Management Response:

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.
Management Action: Remediated

IT continues to provide a weekly report.

Audit Observation: Remediated

IA inspected the weekly IT report sent to the Senior Executive Director of Business for a sample of three weeks from the period of 1/1/17-4/30/17. IA noted that the status of projects and organizational objectives were included in the report as well as help desk metrics that are generated with the help of CBTS.

Observation 4 - Lack of IT Representative in Senior Leadership Team (Medium Risk)

Currently, the Director of Information Technology is the highest-ranking information technology staff member in CCS. No IT personnel are included in the senior leadership team; the Senior Executive Director of Business & Operations serves as the liaison between the Information Technology Department and the senior leadership team.

Recommendation:

Information technology should be part of CCS's strategic objectives and should have direct representation at the senior leadership level. Typically, this representative is a Chief Information Officer or Executive Director of Information Technology. We recommend that CCS evaluate qualified candidates (both internally and externally) and either hire or promote a staff member to represent the Information Technology Department on the senior leadership team.

Initial Management Response:

This recommendation has been shared with the COO and the Senior Executive of Business and Operations to be further evaluated with the senior leadership team.

Management Action: Not Remediated

This is not a decision that can be made in the IT department. Our Senior Executive Director and COO are the voice for IT at the senior leadership level.

Management response remains unchanged.

Audit Observation: Not Remediated

Vendor Management

Observation 5 - PII Data Being Transferred to Third Parties via Unsecured FTP (High Risk)

The following third-party data transfers (and associated PII) were being facilitated via FTP (file transfer protocol, and unsecure means of file transfer that can be intercepted by a third party) instead of SFTP (secure file transfer protocol):

- MEC Library (student data)
- Public School Works (employee data)

FTP is not encrypted and can be intercepted and read by unauthorized entities.

Recommendation:

CCS should immediately disable all data transfers involving PII that are not secured and work with each third party to adopt a secure means of data transfer.

Initial Management Response:

The data transfers in question were disabled immediately. The IT Department worked with Metropolitan Education Council (MEC) (Library Cards) and Public School Works to send the data feeds to a secure, FTP site. All other data feeds followed secure data transfer protocol.

Management Action: Remediated

This was remediated in 2016.

Audit Observation: Remediated

Observation 6 - No Security Guidelines or Minimum Control Requirements in Contracts (High Risk)

CCS does not specify minimum data security guidelines in contracts with vendors. Vendors that process CCS data are susceptible to data breaches that could expose CCS data to unauthorized individuals.

Recommendation:

CCS should require a data security clause in contracts with vendors that are handling CCS data. The clause should require the vendor to prove that it has minimum security controls in place and that reasonable security practices exist to prevent a data breach and unauthorized access and exposure to CCS data. The clause could be included in the General Terms and Conditions or be included separately into individual contracts.

Initial Management Response:

All vendors are subject to the provisions of the Family Educational Rights and Privacy Act.

As well, specific contracts include the following language:

1. The vendor must hold student Personally Identifiable Information (PII) in strict confidence and not disclose PII to any third parties nor make use of such PII for its own benefit or for the benefit of another, or for any use other than the purposes of this agreement.
2. The vendor shall promptly rectify any such breach and shall notify CCS within 24 hours of learning of the breach.
3. At its own expense, the vendor shall notify in writing all persons affected by any unauthorized disclosure of confidential information.

CCS's general terms and conditions also contain the following stipulation and have included this language since at least January 1, 2015:

In the event that CCS shares education records with the vendor, the vendor is subject to the provisions of the Family Educational and Privacy Act regarding the use and re-disclosure of personally identifiable information from educational records included in 34 C.F.R. § 99.33 as well as other requirements established by CCS.
Management Action: Remediated

Audit Observation: Remediated

IA inspected CCS's General Terms and Conditions and determined that it was updated to include specific language around the security requirements for handling CCS data. Also included in the language was a

right-to-audit clause. The General Terms and Conditions must be followed by all vendors of Columbus City Schools.

Observation 7 - No Comprehensive Vendor Review Process (High Risk)

A comprehensive vendor review program is not in place. Criteria for reviewing vendors are not defined and performance reviews are not done regularly or documented when they are performed. A comparison to competing vendors is not performed in order to ensure that CCS is continuing to maximize return on investment.

Recommendation:

CCS should implement a comprehensive vendor review program in all departments (not just IT). The program should first be defined with specific criteria for which vendors can be evaluated. Once CCS has established criteria for evaluation, vendor performance should be reviewed on a scheduled basis (yearly or at end of contract term) to ensure that vendor performance meets CCS expectations and service levels as documented in the contract and SLA. The review should also compare the vendor to competitors and ensure that CCS is getting the best value from the current vendor.

Initial Management Response:

CCS personnel meet with vendor's periodical, as needed, based on the size of the contract, specific needs, performance requirements, etc.

Subpar vendors are monitored on a case-by-case basis. Handling issues on a case-by-case basis is the most efficient method of addressing problems. It utilizes the fewest resources and addresses problems as they occur rather than waiting for a future, scheduled meeting. If the performance of subpar vendors does not improve, that performance is documented and appropriate action taken based on a formal, written process for handling serious vendor issues as prescribed for public entities by the National Institute of Governmental Purchasing. That process is included in CCS's Purchasing Handbook which can be found on CCS's intranet site. If a problem is serious and cannot be rectified with the formal, written process, a "Stop" is placed on the vendor in the vendor database preventing their future use.

Minor issues are resolved in the most efficient manner possible, including phone calls.

Management Action:Remediated

Audit Observation: Remediated

IA inquired of the IT Director and Purchasing Director, and obtained a copy of a completed Vendor Review Form for a contract where the annual value is $500,000 or greater. No exceptions noted.

Management Action:

Vendor reviews for all IT contracts over $500,000.00 were completed at the end of May 2017 and are on file in the Purchasing Department.

Implementation Date: Complete

Observation 8 - No Review of Vendor's Security Controls (Medium Risk)

CCS does not perform any review of the data security environment for vendors that are processing CCS data. The simplest way of performing a review would be through examination of the vendors SOC report. CCS indicated that it has requested SOC reports from vendors, but the vendors decline to share this information due to privacy concerns given that all information shared with CCS becomes public record.

Recommendation:

CCS should implement a process that requires an inspection of the SOC report for all applicable vendors that store or transfer CCS data. The review should occur annually and document any findings found in the report as well as the impact of the findings on CCS operations and data security. In the event that a SOC report is not available for physical distribution, alternative methods of viewing the report should be explored, such as a live-web or on-site viewing.

Initial Management Response:

Vendors are unwilling to provide this documentation to CCS.

Management Action: Not Remediated

Vendors continue to be unwilling to share their complete SOC report.

Audit Observation: Not Remediated

Observation 9 - No Regular Review of Vendor Contracts (Medium Risk)

Contracts and SLAs are not reviewed regularly; reviews generally occur when an issue arises or a decision on the vendor is needed at contract expiration.

Recommendation:

A formal and documented procedure should be put in place where contracts with vendors are reviewed on an annual basis. The contract review should include (but not be limited to) the following:

- The contract conforms to enterprise standards and legal and regulatory requirements;
- The contract continues to be an adequate representation of the services provided by the vendor and the services documented are still relevant to CCS; and
- Necessary improvements are documented, evaluated and communicated to the vendor.

Initial Management Response:

CCS personnel manage contracts on a day-to-day basis including interacting with vendor personnel, addressing issues, ensuring compliance with the contract, and reviewing and authorizing payment of invoices. If improvements are identified, they are analyzed and implemented as soon as feasible.

At this time, implementation of the process recommended by the auditor would not add value and would therefore be a waste of resources.

Management Action: Remediated

Audit Observation: Remediated

IA inspected an agreement for the Infinite Campus contract and noted that Legal approved the contract on 7/8/16.

Observation 10 - Original Vendor Contract Not Available (Low Risk)

Internal Audit inspected the Naviance vendor file at the Purchasing Office and noted that the original contract was not available. Internal Audit did inspect contract extensions/addendums for Naviance, which indicated that a formal contract was initially in place.

Recommendation:

CCS should request the original contract from the vendor and be sure to maintain all contractual documentation for all vendors at CCS facilities.

Initial Management Response:

The Naviance (Hobson's) contract dated August 6, 2014 is on file in the Purchasing Department and has been since it was signed by Stan Bahorek on August 19, 2014.

A replacement contract, that was boarded on August 2, 2016, is in the Purchasing Director's office awaiting filing.

If this finding refers to an agreement that precedes those mentioned above, a Purchase Order was issued to the vendor and served as the contract rather than using a separate, formal agreement.

Management Action: Remediated

Audit Observation: Remediated

Observation 11 - No Documented Legal Approval of Contract (Low Risk)

Contracts that originate from the vendor and not CCS must be approved by the Legal Department. Internal Audit inspected the Infinite Campus contract and noted that it did not have CCS Legal Department approval. Upon further inquiry with Michele VanDyke, Director of Information Technology, we determined that the legal approval was likely verbal or through e-mail communication.

Recommendation:

Since all other vendor contracts inspected did have CCS Legal Department approval, Internal Audit does not believe that a procedural change is needed. However, the Legal Department should inspect the Infinite Campus contract and confirm that the contract meets necessary requirements and CCS guidelines. The approval should be documented in the contract.

Management Response:

This audit finding refers to an expired contract. The current Infinite Campus contract meets all district boarding, legal approval, and signature requirements.

Management Action: Remediated

Audit Observation: Remediated

Observation 12 - No Evidence of RFP or Solution Selection Process (Low Risk)

Internal Audit inspected the vendor files located at the Purchasing Department offices and found no evidence to suggest an RFP was issued or solution selection process was performed prior to the selection of the following vendors:

- SchoolNet: Rhonda Rice, Supervisor of Professional Learning and Licensure, indicated that when the vendor was selected in 2005, an RFP was conducted, but there is no documentation of the RFP or evaluation of other vendors.

- Naviance: Michele VanDyke, Director of Information Technology, indicated that there is no information around whether or not an RFP was conducted for this vendor and that she believes that counselors selected this vendor.

An additional vendor was selected in which the contract was initiated recently in order to ensure adequate coverage of the current purchasing process since the vendor contracts with exceptions began over 5 years ago.

Recommendation:

Internal Audit believes that the vendor selection process that is in place for current vendor contracts is adequate. CCS needs to make sure that all vendors continue to be properly vetted, analyzed, evaluated and compared to competing vendors prior to selecting a vendor.

Initial Management Response:

All IT purchases follow the CCS Purchasing guidelines. Those selected in the audit that were initiated through IT met all of the RFP requirements. Those listed above were not initiated through the IT Department and were referred to the initiating departments.

Response from Rhonda Rice: CCS contracted with Schoolnet in 2005. The RFP was conducted at that time by another department under different leadership. I have only been in this position for two years, and the Schoolnet contract is new to my division beginning with the 2016-17 school year.

Management Action: Remediated

Audit Observation: Remediated

IA inspected the RFP that was issued February 2016 for counseling services. This service was being performed by Naviance at the time this observation was opened.

Observation 13 - No Review of Shared Accounts on CCS-SFTP Site (Low Risk)

Accounts on the CCS SFTP site that are used to transfer data between CCS and other organizations utilize generic accounts that are shared within each organization. While shared accounts generally are not recommended, the nature of the SFTP site makes sense given the nature of each user. However, CCS does not have any controls in place to monitor access to these shared vendor accounts.
Recommendation:

CCS should implement a policy that is sent to vendors with which data is shared via SFTP. Protocols included in the policy should include (but are not limited to) the following:

- Vendors must report to CCS any access changes (terminations, new hires, etc.) that will affect access to the shared SFTP account;
- No representative from a vendor should share the password to the account to any individual not authorized to access the account; and
- Vendors must report to CCS any unauthorized disclosure of the SFTP account credentials.

Additionally, CCS should implement a control that requires a member of CCS Information Technology to send a listing of known individuals with access to the shared account to the vendor and require the vendor

to confirm that the listing is correct and appropriate. This control should be performed at least annually in conjunction with the vendor performance review. An additional measure would be to change the password to the shared SFTP account on a regular basis, although applications that systematically authenticate would need to be considered and evaluated.

Initial Management Response:

The sftp sever is currently set up to use the standard server ssh available. Secure Shell (SSH) cryptographic network protocol or operating network services securely over an unsecured network. The best known example application is for remote login to computer systems by users. Each client is a system user where the user is set to his/her home directory as root, but cannot login directly to the server. The user can only see the directory as a root, but can go no further. IT does inform our vendors verbally not to share passwords and to let us know if an unauthorized user has gained access to the information. However, we will endeavor to create a written policy to address this issue. We will also look at a password change policy within the ftp structure as it affects multiple automated systems.

Management Action: Not Remediated

IT will:

1) Work with the CCS department users that uses the vendor product;
2) Verify whether SFTP account is still used/needed;
3) Collaborate with the CCS department to determine who the vendor contact is;
4) Have questions sent to known vendor contact;
5) Document the users who know the passwords or address any concerns we may have with the number of users;
6) Schedule to change the password(s) prior to July 1, 2017 to allow for the procedure to be shared for the new fiscal year.

IT will develop a procedure that is shared with the vendors and CCS department users requesting that they both notify us when a contact is no longer with the company. The procedure will also indicate that we will refresh the vendor contacts and passwords on an annual basis or whenever is deemed necessary, for whatever reason, to protect CCS data.

Audit Observation: Not Remediated

IA determined that the observation remains open. The management response has been updated since the observation's origin.

IA did obtain an updated list of FTP accounts on the FTP server and noted that some accounts were removed since IA's last review.

Observation 14 - Talend Password(s) Used for FTP Jobs Hard-Coded in the Jobs (Low Risk)

Passwords used for connecting to FTP servers for use in integration with third-party trading partners are hardcoded in the Talend jobs.

Recommendation:

We recommend that the passwords be stored in a secondary, secured (encrypted) file that only Talend can access. Talend has provided guidance for enabling this functionality here:

https://help.talend.eom/displav/TalendOpenStudioforDataIntegrationUserGuide52QEN/7.17+Setting+up+an+FTP+connection

Initial Management Response:

The document sent was for an older version of Talend, which is no longer supported. The application development team is changing from a context mode of employing passwords within Talend to its built-in repository, which is inherently encrypted.

Management Action: Remediated

Audit Observation: Remediated

IA inspected screenshots showing that passwords used for Talend jobs are stored in an encrypted manner.

IT Infrastructure

Observation 15 - User Acceptance Forms Not Required for Non-Fixed Assets (Medium Risk)

Users outside of the Information Technology Department are not required to sign a user acceptance form for non-fixed assets. If the non-fixed assets are damaged or lost by the user, they are not responsible for any cost or repairs. Additionally, there are not sufficient tracking mechanisms in place for both old and new technologies, including the disposition of legacy laptops/desktops and the process for retiring these assets. During an audit of iPads that Northland High School took possession of as part a grant, two were found to be missing.

Recommendation:

Establish a district-wide policy for management of high-value, non-fixed asset items (such as laptops and iPads) to ensure that CCS's investment in these items is being monitored. The policy should include sufficient tracking mechanisms for ensuring that the assets are accounted for and that damage/theft is being tracked and that those responsible are being held accountable.

Initial Management Response:

Board Policy 7530 states - The user of Board-owned equipment shall be fully liable for any damage or loss occurring to the equipment during the period of its use, and shall be responsible for its safe return. Currently, it is the responsibility of the building or department to keep track of assets valued under $500.
Management Action: Not Remediated

Upon review of the MUNIS module, it has been determined that it is not set up in a manner to allow for local management. At this time, the district is still exploring the risk exposure and expected loss associated for items that fall below the Board approved tracking threshold of $500 for controlled assets.

Management response remains unchanged over prior year.

Audit Observation: Not Remediated

Observation 16 - No Formal Tracking of IT Infrastructure Warranty Information (Low Risk)

For critical IT assets and infrastructure (e.g., servers, networking equipment) that are owned and managed by the Information Technology Department, warranty information is not formally tracked to identify assets that are nearly end-of-life or end-of-support status.

Recommendation:

For all existing and newly acquired and/or warrantied assets, create an asset tracking list that includes the asset ID, vendor, acquisition date, and warranty termination date. On an annual basis, formally review and update the list to identify assets that may be in need of servicing or replacement.

Initial Management Response:

IT does not maintain a list of assets separate from the Fixed Asset Department in the Treasurer's Office. We will work with that department to see if warranty information can be added to its current inventory, so that it is managed in a single location for audit purposes. All server equipment is reviewed annually in January or February so that it is included in any necessary third party maintenance agreements, where applicable. The network equipment is maintained in the Smartnet software.

Having a single list for auditing purposes outside of the systems that is currently maintaining would be a duplication of effort and could cause irregularities in reporting.

Management Action: Remediated

Audit Observation: Remediated

IA determined that MUNIS was being used to track assets with values of greater than $500. IA inspected screenshots within MUNIS showing that multiple IT assets being tracked.

IA also inquired of the IT Director and determined that warranty information for IT infrastructure was being maintained by a third-party, SSCS, who also performs maintenance on the devices

Observation 17 - IT Fixed Asset Updates Not Timely (Low Risk)

CCS's fixed asset listing is being updated on annual basis based on information from the general ledger and adjustments sent by the Information Technology Department.

Recommendation:

Better tracking of fixed assets, including proper asset risk management, disposal, depreciation calculation and accounting, requires more frequent updates to the fixed asset register. It is recommended that updates be applied as part of the monthly financial close process.

Initial Management Response:

The annual updating of the fixed asset database conforms to current district policy. Additional staffing would be necessary in order to increase the frequency.

Management Action: Remediated

This was remediated in 2016.

Audit Observation: Remediated

IT Infrastructure

Observation 18 - A Business Impact Analysis Has Not Been Performed (Medium Risk)

The business impact analysis (BIA) is the primary input to a disaster recovery plan. It is critical to determining the IT assets and systems that exist within CCS, their criticality, and the requirements for each in the disaster recovery plan.

Recommendation:

Perform a district-wide BIA, including information technology.

Initial Management Response:

While the Department of Safety and Security has provided some direction and training to several business and operation departments regarding Disaster Recovery, we are also seeking the help of an outside business consultant that will guide through the process of performing a district-wide BIA to include all business and operations departments, including information technology.

Management Action: Not Remediated

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.

Management response remains unchanged over prior year.

Audit Observation: Not Remediated

Observation 19 - Application List in Disaster Recovery Plan Incomplete (Medium Risk)

The existing disaster recovery plan only lists five in-scope IT systems (page 19). In addition, recovery time objectives (RTOs) and recovery point objectives (RPOs) are not clearly defined.

Recommendation:

The disaster recovery plan should include all information technology systems, applications, and databases that would need to be recovered in the event of a disaster, regardless of their criticality and if they are hosted by a third party. RTOs and RPOs should be clearly defined for each.

Initial Management Response:

IT will clearly state the RTO and RPO times in the DR for the systems identified in the plan as mission critical. In addition, IT will survey Senior Leadership to list all of the applications that would need to be recovered and their priority in the event of a disaster that would render the data center a complete loss. The plan will begin to incorporate each system and its associated RTO and RPO, during the annual plan update.

Management Action: Not Remediated

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.

Management response remains unchanged over prior year.

Audit Observation: Not Remediated

Observation 20 - Comprehensive Backup Testing Not Performed (Medium Risk)

Although some backup restorations are performed, a comprehensive and rolling test of backup recoverability is not performed.

Recommendation:

Based on CCS's servers that are in-scope for disaster recovery, develop a rolling test plan to ensure that each server and/or database system is tested for recoverability at least once annually.

Initial Management Response:

This is an excellent recommendation and will be incorporated into the DR Plan.

Management Action: Not Remediated

Audit Observation: Not Remediated

IA inquired of the IT Director and confirmed that there have been no changes to the status of this observation.

Observation 21 - No Data Redundancy Sites (Medium Risk)

Currently, there is no off-site cold, warm, or hot site for redundancy. If the primary Kingswood data center were to go down, there were be no immediate remedy for recovering critical on-premise systems.

Recommendation:

In the short-term, we recommend that the Ft. Hayes data center be closed and CCS use the Kingswood data center as the primary data center and use the Hudson data center and the secondary recovery site for all critical district servers. In the long-term, a cost/benefit study should be performed to determine if using a colocation center is a viable option, both for a production data center and restoration.

It should be noted that CCS's financial application (MUNIS) resides in the cloud and would not be impacted by a disaster at the Kingswood data center.

Initial Management Response:

Data center redundancy (warm or hot site) is certainly the desired DR solution for the Kingswood facility. This will be reviewed through the administrative building assessment that will be conducted in conjunction with CCS's facilities master planning. In the short-term, the Hudson data center would be the site for a drop ship of equipment in the event that the Kingswood facility is a total loss.

It is important to note as well, all but one (Food Services) of the critical systems are hosted or software as a service models, so those could be restored quickly through the associated vendors. The recently purchased storage solution, at both the Kingswood and the Hudson facilities, will allow for restore of all personal and share files at the Hudson location. Equipment that manages the thin desktops (approximately 20,000) would need to be rebuilt at an off-site location. While this is costly equipment and would take some time, it is standard equipment and could be deployed at the Hudson site. Computing would not stop in the school buildings during that time, as there are approximately 30,000 mobile devises district wide. In addition, all schools are now fully voice-quality wireless, and additional mobile devises could be purchased to keep the schools in operation.

Management agrees this is an acceptable risk.

Management Action: Not Remediated

Audit Observation: Not Remediated

IA inquired of the IT Director and confirmed that there have been no changes to the status of this observation.

Observation 22 - SAN Still Being Utilized for File Storage Instead of Office 365 (Low Risk)

Although CCS has adopted Office 365 for cloud file storage, many users are still storing files on the storage area network (SAN). This increases CCS's risk exposure (in the case of a breach) and also impacts the cost and recoverability of these assets.

Recommendation:

Implement a policy requiring that all new content be saved to the cloud. Make the existing SAN read-only and implement a migration strategy for migrating existing content to Office 365.

Initial Management Response:

CCS is moving to cloud storage models. This is an excellent recommendation and one that is being utilized in CCS now with both Office 365 and the Google suite of tools. IT is working to move everything to the cloud, but obviously this will be a process over time.

As we move to all cloud based services, having the SAN in place is critical and management agrees this is an acceptable risk. In addition the SAN will remain necessary for files that are too large for the current Office 365 allotted storage. The SAN is fully redundant and will not be completely abandon.

Management Action:

CCS will not abandon the SAN as a storage option.
Audit Observation: Remediated

IA agrees with management's approach, no exceptions noted.

Physical Security

Observation 23 - Access to the Kingswood Data Center Building Not Sufficiently Restricted (Medium Risk)

Kingswood currently houses the Information Technology staff and data center as well as Accountability, Testing and Assessment and a small group from Special Education. In addition, the building is used as a meeting site regularly by many departments throughout CCS. Many people work in the building outside of custodial hours, often in the early hours of the morning and late at night and all hours of the weekend. The threat of fire hazards from domestic items such as coffee pots, refrigerators, etc. is present. According to the Information Technology Department, the custodian turns off all of these domestic appliances if he is in the building, but occasionally some are left on.

Several years ago, based on an Auditor of State finding, magnetic lock doors were installed to separate the IT spaces from the rest of the building, and the receptionist (front entrance) was moved to the Virginia Ave. side of the building. At that time, the only common areas in the building were the media room, training labs, cafe and the restrooms in that area. The building now houses the Special Education group

located inside the secure area where they receive guests through the King Ave. entrance (without signing into the building). The student information system group is housed in the secure area (to be moving to Central Enrollment at some point).

Recommendation:

Access to the Kingwood data center (including areas adjacent to the data center) should be explicitly prohibited and enforced via access points. Access policies should be developed by the Information Technology Department and enforced within the building.

Initial Management Response:

As the result of an Auditor of State audit, the data center portions of the building were secured with mag locks and card reader access in 2009. In addition, the reception area was moved from the King Ave. facing entrance to Virginia Ave. At that time, public areas in the Kingswood facility were made accessible for training and meetings (labs and the media room). There are currently two non-IT departments inside the secure area; Infinite Campus (which only became part of the Accountability Department in 2015) and a unit of the Special Education group that was displaced when the Neil Ave. facility closed. This has caused additional traffic in the secure areas and needs to be minimized.

Short-Term Plan:

- Notification to district and building staff that only key-card entry is allowed for the King Ave. entrance. All visitors or district staff who do not reside in the secure area are required to enter through the Virginia Ave. (main entrance), sign the building log in sheet and be escorted to any location in the building outside of the designated public areas.
- Access to the conference rooms and offices in the secure area will be used by IT staff only.
- All doors with the mag locks will remain closed at all times.
- Access to the secure areas in the building and the data center will be restricted to those individuals who require access.

Long-Term Plan:

- The Infinite Campus group will be moving to the Central Enrollment facility when the construction of the additional office space is completed.
- The Special Education unit will be relocated to a vacant area in CCS.

Management Action: Not Remediated

Physical security is monitored. IC is moving out of the secure area in the Summer of 2017 and the district is currently looking for space for the special education group to relocate. Once that is complete, there will be no access to the secure areas of Kingswood other than IT staff.

Audit Observation: Not Remediated

Observation 24 - No Raised Floors at Hudson and Fort Hayes Data Centers (Medium Risk)

The data centers at Hudson and Fort Hayes do not have raised floors. This could result to damage to the servers in the event of a flood.

Recommendation:

Given that the Fort Hayes data closet will eventually be removed, the primary risk is to the Hudson data center. We recommend that raised floors be installed as soon as possible.

Initial Management Response:

Raised floor options will be included in the administrative building assessment.

Management agrees this is an acceptable risk.

Management Action: Not Remediated

Audit Observation: Not Remediated

IA inquired of the Capital Improvements Director and determined that the observation remains open.

Observation 25 - No Fire-Suppression Systems in Primary Data Centers (Medium Risk)

Both the Kingswood and Hudson data centers rely on the building sprinkler systems for fire suppression. These are not sufficient for fire suppression and will most likely damage the servers in the event of a fire.

Recommendation:

Implementation of an FM-200 fire-suppression system in the Kingswood datacenter began in June 2016. This fire-suppression system is a clean, colorless, and environmentally friendly fire-suppression agent that is electrically non-conductive. It extinguishes flames primarily through heat absorption, leaving no residue, thus minimizing downtime after a fire. No water or dust is thrown from this system. Recovery of equipment in the data center is maximized, and equipment can be moved from the data center to a different location should the Kingswood facility require significant repair.

Implementation of fire-suppression technology (such as Halon) at the Hudson data center will be reviewed through the administrative building assessment that will be conducted in conjunction with CCS's facilities master planning.

Management is willing to accept the risk.

Management Action: Remediated

Audit Observation: Remediated

IA observed the FM-200 fire suppression system at the Kingswood data center.

2014 AUDIT OBSERVATION REMEDIATION STATUS

Of the 26 observations identified during the 2014 audit, only 10 remained open as-of 2017 (the remediation status of the other 16 was confirmed in 2015). A follow-up audit was performed to determine the status of each, as summarized in the table below.

Observation	Risk Level	Management Action	Audit Observation
IT General Controls			
2. Logical Access - Weak Password Settings or No Password Requirements	High	Application Limitation	
4. Logical Access - No Review of User Access or Roles	Medium	Remediated	Not Remediated
5. Logical Access - No Review of User Activity	Low	Not Remediated	Not Remediated
7. Change Management - No Review of Changes to the Database (Infinite Campus)	Medium	Not Remediated	Not Remediated
8. Job Scheduling - No Procedure or Procedures	High	Remediated	Not Remediated
Network Controls			
1. A Network Vulnerability Scan and Penetration Test Have Not Been Recently Performed	High	Remediated	Remediated
3. Windows XP Machines Still Active	High	Not Remediated	Not Remediated
Human Resources Review			
1. Lack of Continuity in IT Leadership	Medium	Not Remediated	Not Remediated
3. Outdated Job Descriptions	High	Remediated	Remediated
5. Insufficient Staffing to Achieve Desired Control Objectives	Medium	Not Remediated	Not Remediated

Logical Access

Observation 2 - Weak Password Settings or No Password Requirements (High Risk)

During testing, we noted that the food service application (Rightrak) only requires a weak set of password requirements. The settings do not require password history, maximum password age and complexity. Additionally the password length minimum is only one character.

The Transportation application (Versatrans) does not have a password setting standard. A user can log into the application without password credentials.

Recommendation:

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.

Initial 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.

Management Action: Not Remediated

During initial testing, we noted that RIGHTrak and VersaTrans were exceptions due to application limitations.

Audit Observation: Not Remediated

RIGHTrak and VersaTrans cannot comply with procedure due to application limitations.

Observation 4 - No Review of User Access and Roles (Medium Risk)

Aside from Infinite Campus, there is no formal review of user access and roles within the applications to catch any oversights during the initial user request. CCS may not know who has access to an application and the data within. Also CCS may not know if the user's access is appropriate and approved by proper individuals.

Recommendation:

CCS should establish application ownership for each application. Upon establishing business owners (and garnering cooperation of the business), IT can send access lists with user and roles to validate that the user should have access and that the proper role was assigned to the user. The frequency can be determined by CCS, but we would recommend at least annually.

Initial Management Response:

MUNIS: Business owners for each of the core applications within this application suite have been identified; Human Resources, Treasurer's Office, Budget and Procurement. Administrative access to this application suite is managed in the Treasurer's Office. A procedure will be established for an annual review by the core business owners for the accuracy of the access.

Versatrans: Ownership is established for this application; Director of Transportation. IT will be working with the Transportation department to establish an access control policy.

RightTrack: Ownership is established for this application; Director of Food Services. IT will be working with the Food Services department to establish an access control policy.

Talend: is an open source software vendor that provides data integration/feeds to our enterprise software applications. Ownership of this application resides in the application development department in IT. A procedure will be established for an annual review, for the accuracy of the access.

Infinite Campus: While there is a formal review process established for maintaining the access control for the Infinite Campus application, there is not a business unit owner for this application. The IT department currently maintains the standard role access and all additional access must be approved through a formal process (Principal, Executive Director, IT and final approval of the Chief Operations Officer). IT will work with senior leadership to assist with establishing this ownership, so the accuracy of access may be maintained.

Management Action: Remediated

According to CCS IT, a user review has been performed for Infinite Campus, MUNIS, Talend, VersaTrans and Active Directory.
Audit Observation: Not Remediated

Per the 2017 audit results (see observation 3) user access reviews are still not being performed for VersaTrans.

Observation 5 - No Review of User Activity (Low Risk)

There is no evidence of review of log activity. Each application or system has the ability to record login/logout activity. The ability to track and analyze user behavior can be used as a deterrent to inappropriate behavior and can be used as a form of remediation.

Recommendation:

A method should exist to review user activity logs on a periodic basis. Since the logging ability exists within each application, management should determine to what extent the logs needs to be reviewed. It should be noted that capturing information that will not be accessed for review can generate large audit logs that consume resources.

Initial Management Response:

A procedure will be established to monitor activity. An annual review of the software log would not net an auditable result. Each of the systems and their components has peak processing windows. The IT department will work with the business owners to establish a procedure and the appropriate time frames for review.

The only system that does not have a specific lead or owner from the business unit is Infinite Campus. Once that is established IT will work with that group to review monitoring reports that are available in the system.

Management Action: Not Remediated

While monitoring reports have been established for MUNIS, they have not for all systems. IT does not always understand what makes sense to monitor for all systems. IC is likely monitored, business ownership is in the Office of Accountability.

Audit Observation: Not Remediated

IA determined that the observation has been remediated for MUNIS, but remains open for other applications that sit outside of IT. The management response has been updated since the observation's origin.

Observation 7 - No Review of Changes to the Database (Medium Risk)

The ability to make database changes within the Infinite Campus database is limited to the Infinite Campus support team. The area of concern is that the users can make changes the data that potentially allow administrative users to make changes that were not detected. As currently implemented, a process does exist that requires a request form be made to request such changes at the database level. There is no reconciliation of these changes.

NOTE: The state reporting team also has access to run scripts to perform mass-updates of data in the Infinite Campus database.

Recommendation:

While staffing constraints can impact implementing a fully robust change management process,

management should have procedures in place to monitor changes to database, including structures and data.

Initial Management Response:

Change management for Infinite Campus changes will be included in the IT Change Management Procedures and included in the policy and procedure manual.

Management Action: Remediated

According to CCS IT, change management for Infinite Campus is included in the IT Change Management Procedures.

Audit Observation: Not Remediated

We were unable to completely conclude whether all application or database changes are logged. Custom field database changes for Infinite Campus can be queried, but no date/time stamp is available to validate when the change was made. It was confirmed that these change logs did not feature a date/time stamp through inspection of the Infinite Campus custom field report.

Observation 8 - No Procedure or Procedures (High Risk)

There is no overall job scheduling or monitoring policy in the CCS environment. The lack of this policy allows multiple users to make jobs changes. The job scheduling jobs are run from one of three accounts (root-Linux super user account, oracle and k12intel). Since a documented account access list is undocumented, monitoring job changes could be deemed ineffective.

Additionally, Talend jobs responsible for extracting, transforming and loading data across the environment are not governed by formal change control procedures. These jobs, if not managed properly, have the capacity to make erroneous updates to data in all system databases (including MUNIS, Infinite Campus and Versatrans).

Recommendation:

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.

Initial Management Response:

The Application Development group follows the procedure stated when scheduling a new job. This procedure is not formalized in a manual and will be added to the overall IT policy and procedures manual. In addition the manual will include the list of all jobs, and will be updated as job schedules change and will be reviewed annually for accuracy.

1. First we code the job with Talend Open Studio (an open source graphical user interface that allows us to perform complex tasks without having to deal with the technical details).

2. Then we run it locally, verify its results until it meets what we think that the client wants.
3. Then we commit the generated source to source control so that we do not lose the work.
4. Then in Talend Open Studio we run an export utility that packages the job and also creates a Linux/or Windows executable file depending on the desired target system.

5. We FTP the packaged job and its executable to the server.
6. Create a Cron entry with the desired time of execution and the frequency of run.
7. Notify the client that the job has been deployed and that it will run at the specified time. If the client encounters an issue or an enhancement needs made, we repeat steps 1 through 5.
8. Jobs usually have exception handling so that if any component within it fails we get an email so that we can be proactive instead of waiting for the customer's call.

Management Action: Remediated

We do have an overall job scheduling and monitoring process and server. Only vendors that have signed an MUP with the district can have jobs on the job scheduling server. All other jobs are disabled. We are informed that if the vendor has one signed and see a copy of it prior to setting up the job. Job scheduling jobs are ran from a non-privileged user and NOT root. Oracle, k12intel connections are contained inside the job and are encrypted. All job changes must be created as a Talend job and can only be done by one of three individuals. Talend is used to create the framework of the job and IS NOT the job itself or where it runs. All jobs DO NOT update data. They are designed to EXTRACT data, TRANSFORM the data, and LOAD it into spreadsheets and text files that are sent to outside vendors (thus the name ETL). ETL jobs DO NOT change the data in Infinite Campus or Munis or Versatrans. The ONLY databases modified by any job are CCS owned and created databases.

Audit Observation: Not Remediated

IA inquired of Alex Smith and Shawntel Lewis and determined that a process appears to be in place for job schedule administration. However, it is not documented in a formal job schedule or procedure and does not include the opening of a ticket for development of new jobs or modification of existing jobs.

IA noted that Alex Smith, who is primarily responsible for the administration of scheduled jobs, does perform a due diligence check to determine if an MUP has been signed with the vendor. For a sample of three jobs, IA did obtain the contract for that vendor to determine an MUP was in place. Alex Smith also follows-up with any jobs that request sensitive information.

Network Architecture and Security

Observation 1 - A Network Vulnerability Scan and Penetration Test Has Not Been Recently Performed (High Risk)

The most recent network vulnerability scan and penetration was performed four years ago and was paid for by the State of Ohio. Such scans are crucial to assessing the effectiveness of existing network security protocols and for identifying critical vulnerabilities in the network and system configurations.

Recommendation:

Given the relatively low cost of performing these scans it is recommended that a network vulnerability scan and penetration test be performed annually.

Initial Management Response:

The audit team with Schneider Downs provided information regarding a firm that can perform this test. The IT department will use this firm in the summer of 2014. We will also look into other potential companies, so that we can use a different firm every couple of years.

Management Action: Remediated

A vulnerability scan and penetration test was performed by a third-party in 2016.

Audit Observation: Remediated

IA observed the results of the vulnerability scan dated 4/16/16 to determine that vulnerability tests were performed. IA also inspected a summary provided in order to determine remediation status of the vulnerabilities detected. For a sample of 5 vulnerabilities that had been noted as remediated by IT, IA obtained evidence to support actions taken to verify remediation.

Observation 3 - Windows XP Machines Still Active (High Risk)

Upon inquiry it was determined that some Windows XP machines are still active and running on the network. Microsoft is terminating support for XP on April 8, 2014. Therefore, any new vulnerability discovered in the operating system will not be addressed/patched, and could expose the school district's network to the risk of malicious attack.

Recommendation:

Retire/replace existing Windows XP machines prior to April 8.

Initial Management Response:

Like many school districts throughout the country, Columbus City Schools (CCS) does have computers still running the Microsoft Windows XP operating system (OS). CCS takes the end of support for Windows XP very seriously and has been taking steps to move the district to the more modern Microsoft Windows 7 OS. The district faces many challenges to making this move to a new platform. Many of the software titles in use today are not supported and/or perform poorly on a Windows 7 based computer. Additionally, a large number of computers in the Columbus City Schools fleet are 8 plus years of age and cannot be upgraded to this new OS without moving to our virtual desktop infrastructure (VDI).

Columbus City Schools has been planning for the move to Windows 7 for several years now. We have been testing compatibility of applications and have been piloting users on the updated operating system. In addition, CCS has installed one of three phases of a new Virtual Desktop Infrastructure (VDI) utilizing servers on the Cisco USC platform and a Citrix based virtualize software environment. This new environment provides users with a virtual Windows 7
OS experience.

To date, CCS has upgraded the computer labs at all high school and middle schools in the district. CCS has upgrade 43 elementary school computer labs and additional 20 plus laptop cart labs to either Windows 7 or to our new VDI environment. In regards to administrative users, CCS has recently completed the conversion of the downtown Columbus Education Center (CEC), and will be completed with the upgrade of the remaining administrative locations by the end of the school year.

CCS will be acquiring hardware for the completion of phase two of the new Virtual Desktop Infrastructure (VDI) in May. The phase two deployment will allow us to convert an additional 3000 teacher computers to new environment. Planning is also underway for phase three of the VDI deployment. Phase three should allow CCS to convert an additional 3000 teachers computers and the remaining student computers to the new virtual environment. There will most likely be some users that either will need new computers or will need to remain on Windows XP to utilize software that cannot

be upgraded or replaced.

It should be noted that even though Microsoft has ended their updates to Windows XP, our antivirus software provider Sophos, has stated that they will continue to support Windows XP updates until sometime in 2015.

Management Action: Not Remediated

Updated Management Response: The district still has a small number of XP machines in operation (approximately 4). All of the current XP machines are running software that has not been upgraded to a newer version of the operating systems or is running a software where the browser must remain at a lower version.

The IT department will provide a list of the machines to senior leadership to determine the steps to remediate this finding.

Audit Observation: Not Remediated

Human Resources

Observation 1 - Lack of Continuity in IT Leadership (Medium Risk)

The CIO is responsible for establishing the objectives and direction of the IT organization and ensuring alignment with organization objectives. CIO leadership and continuity is a critical component of IT success. A lack of continuity can result in conflicting objectives, misdirected resources and undesirable service levels/outcomes.

Recent CIOs at CCS have had limited tenures and have not persisted long enough to make a meaningful impact. Currently the role of CIO is vacant; the IT Operations Manager is serving as interim CIO and there has not been an attempt to fill their prior, vacant position.

Recommendation:

CCS should perform a thorough search for IT leadership (both internal and external) and fill requisite positions with individuals that 1) are committed to the vision and direction of CCS, 2) are committed to using technology to improve student outcomes, 3) can demonstrate effectiveness at leading IT organizations and aligning IT to business objectives, and 4) have a proven track record of longevity at prior organizations.

Initial Management Response:

In the past twelve years there have been eight changes in the CIO position. In addition to the reasons stated by the auditors, this also results in focus, vision and initiative change, lack of confidence by the customer and the internal staff is left feeling uncertain, resulting in low morale. In March 2014, a decision was made not to fill the CIO position for the time being and the Interim CIO was moved to the Director of Technology.
Management Action: Not Remediated

In March 2014, CCS decided not to fill the CIO position. Instead, the Director of Technology will serve as the lead for CCS IT.

Audit Observation: Not Remediated

Although a clear chain of command and leadership role to have been assigned for CCS IT, the absence of a CIO role is still a risk given the size of CCS and the necessity for such a role to effect change within the district, as well as to provide the level of visibility necessary within the state of Ohio.

Observation 3 - Outdated Job Descriptions (High Risk)

The current job descriptions that are approved in place (both for existing employees and new hires) do not reflect current roles, responsibilities or qualifications. As an example, the Data Processing Analyst position (Appendix C) lists COBOL programming experience as a desired skill and also states that an associate's degree is the minimum education qualification. COBOL is no longer used at the department and, as a whole, is an antiquated language. Finding and retaining qualified candidates will be difficult if job descriptions do not maintain pace with current needs and technologies. Reference Appendix D for an example of a current job description that reflects the actual needs of the organization.

Recommendation:

Revise both internal job descriptions for existing employees (to ensure staff alignment with needs) and for new external job postings.

NOTE: A similar project was underway within the Human Resources department but was put on hold by CCS leadership in favor of other projects.

Initial Management Response:

Human Resources Management Response: As an outgrowth of the job description revisions work that began in the IT department, a district- wide class specification (a.k.a. job descriptions) update plan is being developed in partnership with the Columbus Civil Service Commission. Once the update plan is developed and approved by the Columbus Civil Service Commission, the revision and submission of class specifications for approval by the Columbus Civil Service Commission will begin. The IT class specification updates being prioritized accordingly.

IT Management Response:

The IT position descriptions that are currently assigned to employees were written at least 30 years ago. This was an audit finding with the state auditors in the annual IT audit for at least five years. This finding was removed from the IT audit two years ago as the job descriptions were re-written and transferred to the HR department.

In 2008, the IT department, with the approval of HR, agreed to re-write all of the IT job descriptions. This process continued annually from 2008-2012. The job descriptions have been re-written, updated to reflect current needs and reviewed by employees for input. HR has all of the job descriptions and has been working on a project over many years to have all of the job descriptions in the district updated, compensation assigned and approval through civil service where appropriate.

Management Action: Remediated

New job descriptions were developed and posted in 2016.

Audit Observation: Remediated

IA inspected documented job descriptions for a sample of five IT positions to determine that job descriptions have or are in process of being updated to reflect current requirements and responsibilities.

Observation 5 - Insufficient Staffing to Achieve Desired Control Objectives (Medium Risk)

CCS IT is not sufficiently staffed to maintain the level of control necessary to properly mitigate risk. This is especially true in the areas of change management and logical access. Current staff size does not permit for appropriate segregation of duties or oversight of key processes. Many changes are made to environments with limited or no oversight (including program changes that can make direct changes to data).

Recommendation:

CCS should consider consolidating disparate processes across systems (e.g. change management, user provisioning) and using a standard methodology for each. Staff can then be assigned to be responsible for change control/deployment and user access control, independent of the individuals requesting/making changes.

Initial Management Response:

The staff size in the Application Development group has gone from 24 FTEs to 14 in the last five years due to budget reductions and moves to other areas of the district. The group has shuffled many times to support each other in implementation of new software systems and to meet the needs of managing all of the district applications. IT management is continually working to re- align staff to meet all of the needs more efficiently.

Management Action: Not Remediated

Most of the open positions have been filled and the application development area is aligned to programming areas. This is still a very small staff, but they are working in an agile framework to meet the needs of the district.

Audit Observation: Not Remediated

APPENDIX A - 2017 LOGICAL ACCESS APPLICATION SCOPE

The following is the list of applications that were included in the scope of 2017 logical access testing:

- VPN
- Active Directory
- Office 365
- Infinite Campus / OLR
- KRONOS
- MUNIS (TRS, TCM, Vendor/Employee Self-Service)
- Lotus Notes
- Food Service (First Track & Right Track)
- Certify
- Education Mgmt. Info System (EMIS)
- Data Warehouse (VersaFit)
- CIMS (Schoolnet)
- Versa Trans
- CNP (Charter/Non-Public) Database
- Central Enrollment Center
- VFA/FAMIS
- Talend
- CCSDAS
- ADM2000
- Netview
- LobbyGuard

APPENDIX B - CCS DASHBOARD ANOMOLIES

Below is a summary of anomolies identified in reports for the CCD[2] and Financial Dashboards.

CCSD[2]

(http://ccsdashboard.eastus.cloudapp.azure.com/viewer/content/dashboard.html)

Observation #1:

District-wide attendance percentage (April 3-7 2017) for American Indian/Alaskan Native students is 182,820.00%

Management Response:

This gauge on the dashboard shows 100% for April 3-7, 2017 time period as of August 14, 2017.

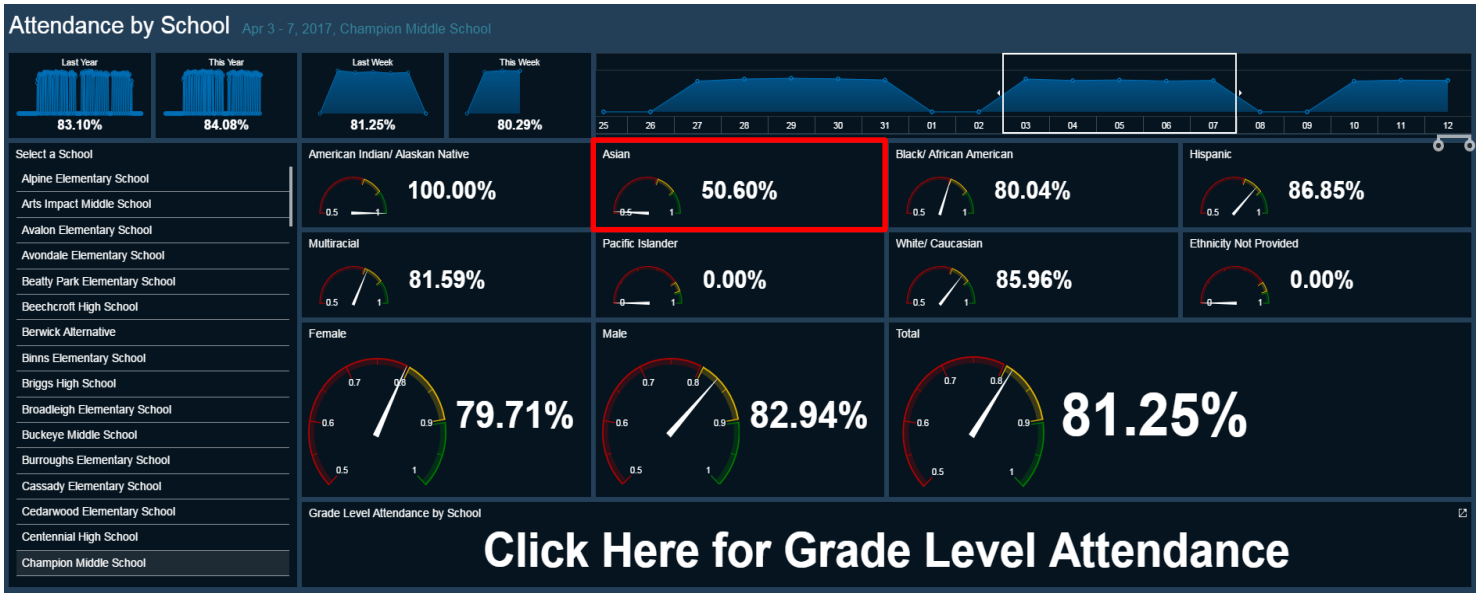
After conferring with the application developer responsible for developing the query and respective job used to gather and process this data, it was determined that there was a coding error associated with the observation. This has since been corrected and new code has been developed, tested, and put into place.

Observation #2:

There is one student classified as "Asian" enrolled at Champion Middle School (evidenced below) between April 3 and April 7 of 2017. Depending on how this page is calculated, 50.60% of reported attendance may be incorrect.

Management Response:

387 minutes per day * 5 days = 1935 minutes. This student missed 150+52+387+387 = 976 minutes. 976/1935 = 50.43%. This is indeed calculated correctly. While the data has slightly changed due to the processing of attendance documentation, you can see that the CCSD² result is an exact match to the single student in that student group as calculated directly in the IC ADM/ADA stored procedure and report. There is no error present.



Financial Dashboard

(http://transparency.tylertech.com/ccsoh/pages/Default.aspx?PageView=Shared)

Observation #3:

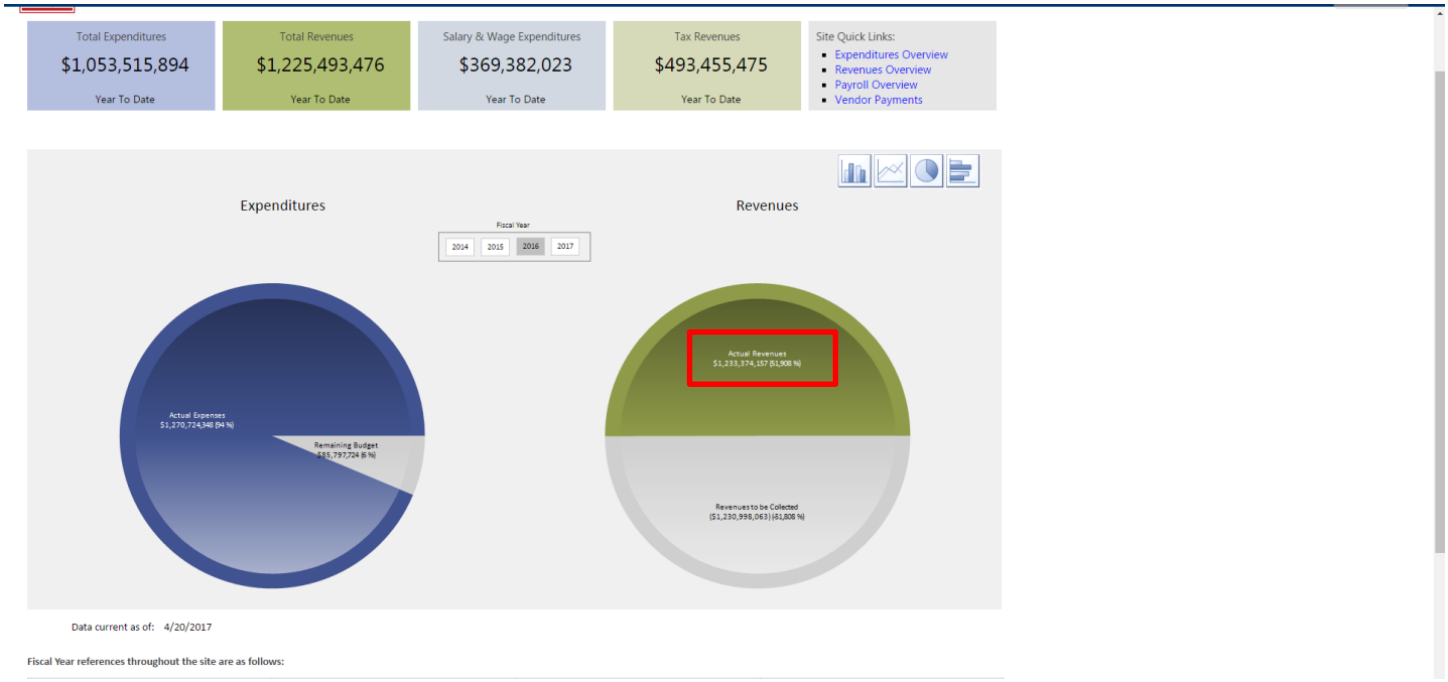
Pie charts for 2014 and 2015 Revenue show half as being collected, half as being uncollected and the corresponding percentages as "Infinity" and "-Infinity"

Management Response:

These were developed by Tyler Technologies and were not identified during testing due to differences in how data is stored by CCS versus how it was expected by Tyler.

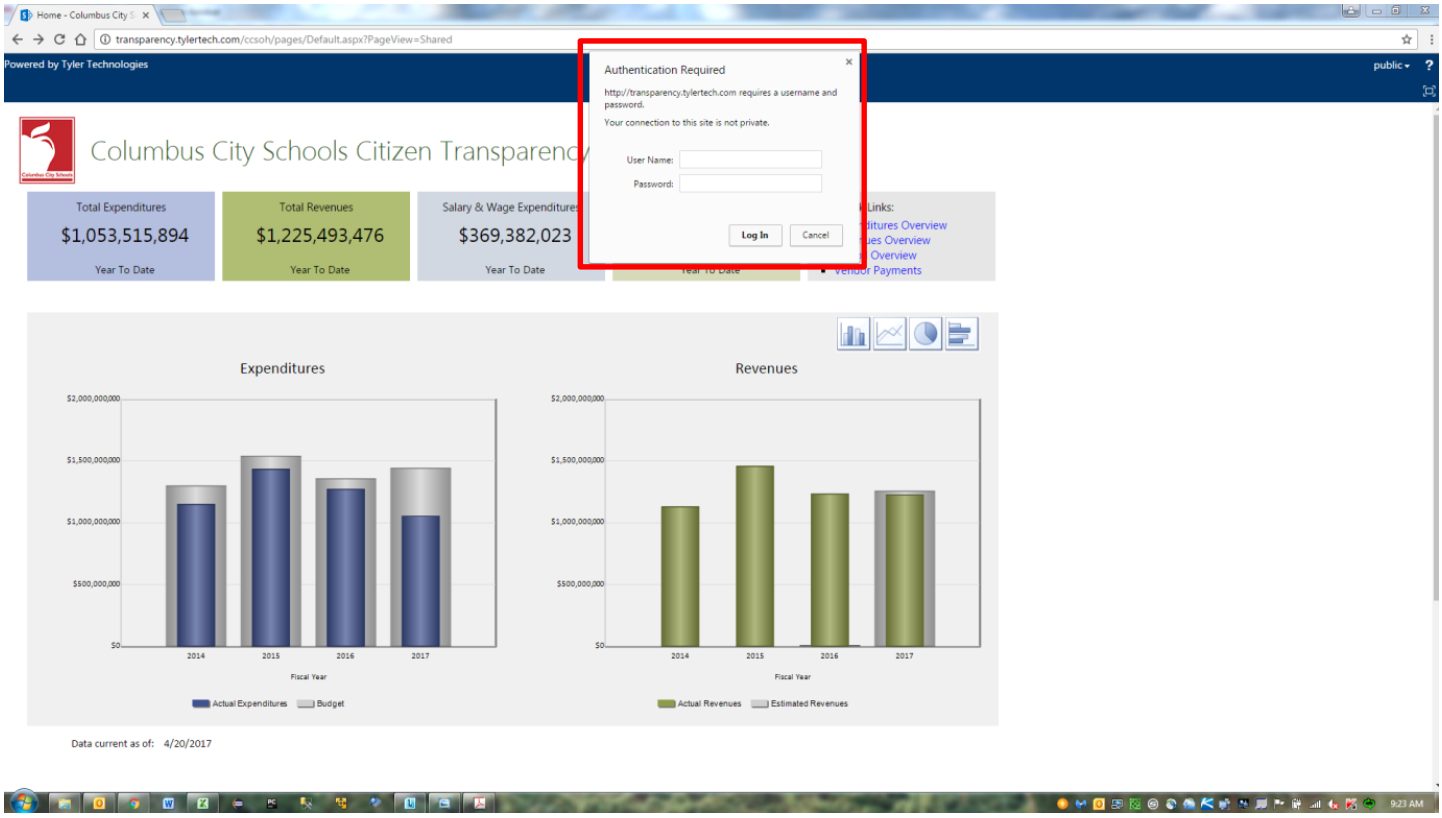
Observation #4:

2016 pie chart for revenue shows percent of revenue collected as 51,908% and uncollected as -51,808%



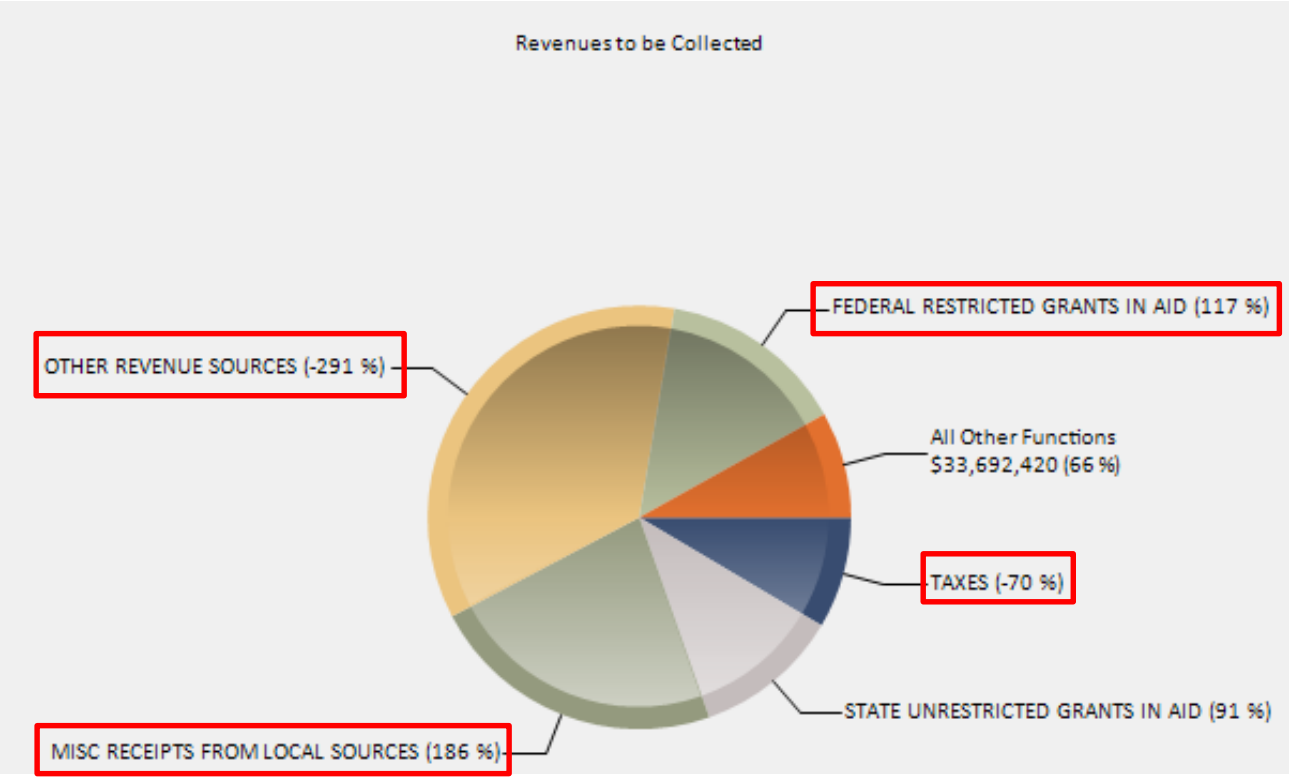
Observation #5:

Chrome asks for authentication but clicking the "X" to close it out a few times results in it just disappearing and allowing access.



Observation #6:

Revenues to be collected in 2017: Total pie graph adds to 99% but multiple percentages are larger than positive or negative 100.



Observation #7:

Pie charts breaking down actual revenue and revenue to be collected from 2014 show the same graphs but have different numbers. Example: taxes accounts for 39% of actual revenue and 46% of revenue to be collected but the graphs are still identical. "All other functions" is representing -9% of revenue to be collected.