CORTLAND ENLARGED
CITY SCHOOL DISTRICT

INTERNAL AUDIT

RISK ASSESSMENT UPDATE
AND
ANNUAL TESTWORK

July 13, 2021

TABLE OF CONTENTS

D'Arcangelo & Co., LLP
Certified Public Accountants & Consultants

200 E. Garden St., P.O. Box 4300, Rome, N.Y. 13442-4300
315-336-9220 Fax: 315-336-0836

Board of Education and Audit Committee
Cortland Enlarged City School District

We have been engaged to assist Cortland Enlarged City School District in performing an initial risk assessment and annual test work for the year ended June 30, 2021 as required by Chapter 263 of the Laws of New York State. The purpose of our engagement is to assist the District in determining the level of risk and adequacy of controls in the various functional processes within the school district. A complete description of the methodology used in performing the risk assessment is included in the subsequent pages of this report. We have also performed test work in areas agreed to by the audit committee as required. The results of that test work have been included in this report.

The risk assessment and testwork was performed in accordance with professional and ethical standards contained in Government Auditing Standards issued by the Comptroller General of the United States and the general standards of the AICPA's Code of Professional Conduct. These standards are required by the Regulations of the Commissioner of Education.

The engagement to perform the initial risk assessment and test work is part of an ongoing internal audit function. The results of the risk assessment and test work performed have been discussed with management of Cortland Enlarged City School District and are the overall responsibility of the School District.

This report is intended solely for informational purposes in order to develop a plan to identify and manage the School District's risks. This report and all information used to compile the report is the property of Cortland Enlarged City School District.

We appreciate the opportunity to serve you as internal auditors and thank the individuals in your School District for their cooperation.

D'Arcangelo + Co., LLP

July 13, 2021

Rome, New York

METHODOLOGY

The internal audit process for Cortland Enlarged City School District has been established in accordance with Chapter 263 of the Laws of New York State to provide an independent, objective assurance and consulting activity designed to add value and improve the organization's operations. It helps the school district accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Defining Audit Universe

The first step leading to the development of the School District's Risk Register is to define the audit universe. The School District's audit universe encompasses both financial and non-financial functions and has been categorized into the following business units:

- Governance
- Information Technology
- Budget
- Financial Reporting
- Payroll/Human Resources
- Accounts Payable
- State Aid
- Attendance
- Capital Projects
- Special Aid Programs
- School Lunch
- Fixed Assets
- Transportation
- Cash Receipts/Billing
- Extraclassroom

Weighting of Business Units

The risk that each of the above business unit's pose on the School District is unique. The weighting of business units attempts to account for the relative measure of importance between business units and the impact on the overall risk level. A weighting factor was derived by evaluating each business unit based on the following categories:

- *Size of Unit* - Based on total revenue/expenditures processed by business unit band/or volume of transactions.
- *Complexity of Transactions* - Based on the nature of transactions processed.
- *Public Exposure* - Based on the potential of business unit to harm the School District's reputation within the community.
- *Time Since Last Audit* - Based on the last date that internal audit procedures have been performed.

METHODOLOGY

- *Compliance with laws and Regulations* - Based on laws and regulations that direct the business unit's activities.

Defining Business Unit Processes

Business units have been broken out into key processes that will be the basis of the risk register. The objective is to identify and prioritize processes that pose the greatest potential risk and liability to the School District.

Categories of Risk

Risk will be assessed for each business unit process in two categories:

Inherent Risk - Inherent risk measures the potential for objectives not being attained at the desired level before applying the assessment of the internal control process.

Control Risk - Control risk measures the adequacy of internal controls designed to reduce the inherent risk within the process. Each process will be assessed for control risk utilizing the concepts of the COSO model. This model was developed in 1992 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and has been adopted as the generally accepted framework for internal control and is widely recognized as the definitive standard against which organizations measure the effectiveness of their systems of internal control. The COSO model focuses on the following components:

- *Control Environment* - The Control Environment sets the tone of an organization, influencing the control consciousness of its employees. It is the foundation for all other components of internal control, providing discipline and structure.
- *Risk Assessment*- Risk Assessment is the identification and analysis of relevant risks to the achievement of the School District's objectives, forming a basis for determining how the risks should be managed.
- *Control Activities* - Control Activities are the policies and procedures that help ensure management directives are carried out. Control activities include a range of activities such as approvals, authorizations, verifications, reconciliations, security of assets, and segregations of duties.
- *Information and Communication* - Information must be identified, documented, and communicated in a form that enables employees to carry out their responsibilities.
- *Monitoring* - Monitoring is a process that assesses the quality of an internal control system's performance over time.

METHODOLOGY

Assessing a Risk Level

The assessment of risk will be based on four levels of severity:

Low	Low likelihood of significant impact on School District objectives.
Moderate	Moderate likelihood of significant impact on School District objectives.
High	High likelihood of significant impact on School District objectives.
Severe	Extreme likelihood of a catastrophic impact on School District objectives.

Risk Appetite

Risk Appetite broadly sets the level of risk that the Board of Education deems acceptable. The Board of Education has set a *moderate* level of risk appetite for the purpose of this initial risk assessment. Those processes that have been assessed a level of control risk greater than the risk appetite are to be included in the School District's long-range internal audit plan over a four-year period. The level of risk appetite is designated with a blue line on the School District's Risk Register on Pages 5 through 8.

Managing the Risk

The options of the School District in managing its risks can be summarized as follows:

- *Treat* - Implement accounting and operational controls.
- *Terminate* - End the activity.
- *Transfer* - Outsource activity or obtain insurance.
- *Tolerate* - Accept risk and monitor.

Audit Plan

An audit plan must be implemented by the Audit Committee based upon the identified risks, risk appetite, and how the risk is to be managed. Risks identified that are above the acceptable risk appetite of the Board of Education should be a priority in the audit plan.

RISK REGISTER AS OF July 13, 2021

Business Unit	Process	Risk Assessment Update								Testwork Performed					
		Inherent Risk				Control Risk									
		As of July 13, 2021													
		Severe	High	Mod	Low	Severe	High	Mod	Low	2017	2018	2019	2020	2021	Reference
Governance	General Policy and Procedures	✓					✓								
	Monitoring	✓						✓							
	Organizational Structure	✓						✓							
	Risk Management	✓						✓							
Information Technology (IT)	Governance/Security		✓				✓			✓				✓	
	Financial Application Security		✓					✓		✓				✓	
	Network Security		✓					✓						✓	
	Miscellaneous Application Security		✓					✓		✓				✓	
	Disaster Recovery		✓					✓		✓				✓	
Budget	Development	✓						✓							
	Presentation/Compliance	✓						✓							
	Monitoring	✓						✓							
	Amendments			✓				✓							
Financial Reporting	Monthly Reporting	✓						✓							
	General Accounting		✓					✓							
	Annual Reporting		✓					✓							
	Financial Oversight		✓					✓							
	Fund Balance Management		✓					✓							

RISK REGISTER AS OF July 13, 2021

Business Unit	Process	Risk Assessment Update								Testwork Performed					
		Inherent Risk				Control Risk									
		As of July 13, 2021													
		Severe	High	Mod	Low	Severe	High	Mod	Low	2017	2018	2019	2020	2021	Reference
Payroll/HR	Payments to Employees	✓						✓					✓		
	Allocation of Expenditures	✓						✓							
	General Employee Administration		✓					✓					✓		
	Employee Benefit Administration	✓						✓							
	Employee Attendance	✓						✓							
	Hiring/Termination of Employees		✓					✓					✓		
Purchasing/AP	P.O. System		✓					✓							
	Payments Outside P.O. System	✓						✓							
	Procurement Process	✓					✓								
	Private Purpose Trust Expenditures			✓				✓							
	Reporting Requirements		✓					✓							
	Allocation of Expenditures	✓						✓							
	Payment Processing	✓						✓							
	Petty Cash Administration			✓				✓							
State Aid	General Processing/Monitoring		✓					✓							
	Basic Aid		✓					✓							
	Transportation Aid			✓				✓							
	Building Aid/Capital		✓					✓							
	Excess Cost Aid			✓				✓				✓			
	BOCES			✓				✓							

RISK REGISTER AS OF July 13, 2021

Business Unit	Process	Risk Assessment Update								Testwork Performed					
		Inherent Risk				Control Risk									
		As of July 13, 2021													
		Severe	High	Mod	Low	Severe	High	Mod	Low	2017	2018	2019	2020	2021	Reference
Attendance	Tracking Student Attendance		✓					✓							
	Student Performance Data			✓				✓							
Capital Projects	Planning		✓					✓							
	Monitoring		✓					✓							
	Completion		✓					✓							
Special Aid	Grant Application		✓					✓							
	Allowable Costs		✓					✓							
	Cash Management			✓				✓							
	Reporting and Monitoring		✓					✓							
	Compliance		✓				✓								
School Lunch	Federal & State Reimbursement		✓					✓							
	Sales Cycle and System		✓					✓							
	Inventory and Purchases		✓					✓							
	Eligibility Verification			✓				✓							
Fixed Assets	Acquisition and Disposal		✓					✓							
	Compliance			✓				✓							
	Inventory		✓					✓							

RISK REGISTER AS OF July 13, 2021

Business Unit	Process	Risk Assessment Update								Testwork Performed					
		Inherent Risk				Control Risk									
		As of July 13, 2021													
		Severe	High	Mod	Low	Severe	High	Mod	Low	2017	2018	2019	2020	2021	Reference
Transportation	Fleet Maintenance			✓				✓							
	Risk Management		✓					✓							
	Personnel Compliance			✓				✓							
	Facilities Maintenance and Security		✓					✓							
Cash Receipts/ Billing	Real Property Tax	✓						✓							
	Medicaid		✓					✓				✓			
	Out of District Tuition			✓				✓							
	Use of Facilities			✓				✓							
	Admissions and Concessions		✓					✓							
	Donations			✓				✓							
	Collection/Posting of Receipts		✓					✓							
Extraclassroom	General		✓					✓			✓				
	Cash and Cash Receipts		✓					✓			✓				
	Expenditures and Purchasing			✓				✓			✓				
	Inventories			✓				✓			✓				

PRIOR YEAR RISKS AND RECOMMENDATIONS

Governance-General Policy and Procedures

2015-01 *Accounting Procedures Manual*

Current Year Status:

The District is in agreement with this recommendation and has started to compile business office procedures into a google shared folder.

Prior Year Observation

Although the District has documented in limited circumstances certain procedures within the business office, the District does not have a formalized accounting procedures manual or an inventory of its internal controls.

Prior Year Risk

Without documented accounting procedures or an inventory of internal controls, employees have no formal guidance as to their specific role in the accounting process as well as their specific role in the internal control process for the District. An effective internal control system relies heavily on a formal communication system that sets the expectations of its employees and establishes their role in the process. This lack of formal communication increases the risk of internal controls not being followed as intended and an employee not knowing what is expected of them. It prohibits the ability to effectively train new employees, evaluate performance, and improve on existing procedures or internal control.

Prior Year Recommendation

We recommend that the District develop a comprehensive accounting procedures manual that is separate from Board Policy. Such a procedures manual would ensure that procedures are consistently applied throughout the District. It would effectively notify all accounting personnel of their duties and improve lines of communication. In developing the accounting procedures manual, the District should consider the following elements:

- Written job descriptions for each accounting position. These descriptions should be provided to each employee and serve as a guideline for hiring and evaluating personnel. The District already has many of these job descriptions documented.

- Appropriate descriptions of all financial policies, accounting procedures, internal controls over payroll, cash disbursements, and cash receipt cycles.

- A segregation of duties matrix for each of the main transaction cycles that provides an overview of the role of each position in the internal control process.

PRIOR YEAR RISKS AND RECOMMENDATIONS

- A list of standard forms and system generated reports used in the School with a detailed explanation of their purpose and preparation.

The accounting procedures manual should be updated annually and should be distributed to all accounting personnel and other appropriate personnel. It should evolve to meet the needs of the District and should provide an accurate reflection of the current system of accounting.

Information Technology – Governance/Security

2018-01 *Vendor Management*

Current Year Status

The District has reviewed and accepted the recently completed CNYRIC SOC report.

Prior Year's Status

A SOC audit was previously completed of the CNYRIC service organization which covered the testing period ending November 30, 2018. A SOC 2 and SOC 3 reports were issued but CNYRIC only shared the SOC3 reports to the Districts. The SOC 3 report only provides general information with no description of tests performed or the results from the testing. CNYRIC has indicated that a recent SOC audit was completed of the CNYRIC service organization which covers the testing period ending December 31, 2019, in which the SOC 2 and SOC 3 reports will be issued Summer 2020.

Previous Year' Observation

The District is reliant on third parties to operate critical applications in use at their facilities. In order to assess the effectiveness of the controls within these externally hosted operations, it is industry best-practice for these hosting vendors to undergo an independent control evaluation such as the AICPA's Statement on Standards for Attestation Engagements No. 18 (SSAE 18) and Attestation Standards Section 101 (AT Section 101) in order to provide visibility within these service providers' control design.

The District utilizes the *nVision IS* application to handle financial processing (i.e., payroll, vendor check disbursements and maintaining the general ledger) and *IEP Direct* to handle its Special Education program. These applications are hosted by *BOCES (CNYRIC)* along with providing the District's internet access and website. *BOCES* has complete responsibility for managing the application, network connectivity, system operations and security. *BOCES* has not provided a service auditor's assurance report.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Prior Year Risk

The manner in which security over the District's data, hosted at these 3rd party vendors facilities, will not be completely understood or independently validated.

Once these reports are completed, we recommend the District request a copy of the SOC 2 report in order to complete an evaluation to determine 1) whether the report covers all of the services they utilize, 2) identify controls that the District needs to establish which have been delegated by the service organization to the user organizations (i.e., Districts). CNYRIC has indicated that the Availability Trust Service Criteria was not included within the scope of the current SOC audit. However, the CNYRIC has formally represented that they have established offsite recovery capabilities for the application systems that the District uses at the CNYRIC in the event their primary hosting site is inoperable.

Information Technology – Governance/Security

2015-04 *Data Classification*

Current Year Status

This initiative will be completed during the next school year as part of the implementation of the NIST framework as required by ED 2 Part 121.

Prior Year's Status

The District's efforts to complete ED 2 Part 121 will include the classification of PII data which includes establishing the required security controls. This is an ongoing process.

Previous Years' Observation

The District has not developed a data classification standard to classify the risk level of data resources used within the District. Establishment of a data classification standard provides the basis for ensuring that proper levels of controls have been implemented based on the classification of the data.

Risk

Individual users will not have the awareness needed to preserve the overall system security.

Previous Years' Recommendation

A security risk assessment should be established to classify the risk relating to all critical District data. This risk assessment would then be used as the basis of ensuring all District data is properly secured with the required level of separation of duties and controls.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Information Technology – Governance

2015-05 *Records Retention of Student and Business Records*

Current Year Status

The District will be establishing an initiative during the next school year to determine their interpretation of ED-1 data retention requirements and implement the required solutions.

Prior Year's Status

The District's Business Official attended a seminar by the State to obtain guidance on ED-1 and is working toward implementing a records retention program to achieve compliance. We recommend that IT also perform an evaluation of the ED-1 requirements to identify the system users access records, computer system security records and computer usage files that need to be retained along with identifying enhanced storage capabilities that may be required.

Previous Years' Observation

The State of New York has enacted a series of mandates for retention of student and business data (titled ED-1), detailing requirements for numerous types of scenarios and the length of time such records must be retained for both paper documents and electronic records. Formal policies have not been enacted within the District, and specific retention and disposition schedules for each category of data have not been established based on meeting the ED-1 requirements.

Risk

Records required by state regulators, courts, and other bodies may be unavailable, exposing the school to legal action or adversely impacting current or former students or their families.

Previous Years' Recommendation

Obtain and review the New York State mandates. Enact a policy to adhere to these standards, at a minimum. Appoint a records custodian to handle retention and disposition, and periodically review retention for continued compliance. Monitor the regulations for any changes in requirements going forward.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Information Technology-Disaster Recovery

2015-06 *Contingency Plan*

Current Year Status:

Development and evaluation of the Disaster Recovery Plan is being viewed from the standpoint of where business systems are hosted and the means of reaching them in the event of a primary site failure. Presently, only two significant items hosted at the main building are the Transfinder transportation system and the Domain Controller with Active Directory to authenticate to the School Tool student information system. With Transfinder being replaced by a cloud version and Google Authentication being established for School Tool authentication, both this summer, these risks will be eliminated at the main building.

The SAN (Storage Area Network) and virtual servers have been installed at the Smith location which serves as the alternate processing facility. Daily backups are produced which replicate the primary data to this location. All school buildings have connectivity to Smith.

The District is researching means of establishing cost effective outbound internet connectivity to enable access to all key District systems in the event of primary site failure.

The District should identify the potential failure scenarios and develop and perform tests to ensure the viability of alternate processing methods. The Business Impact Analysis also needs to be completed to identify critical business functions and set recovery priorities in the event of an outage to mitigate the potential impact. Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) also need to be developed. The District has elected to *tolerate* the remaining risks related to this area. No corrective action is necessary.

Prior Year's Status

The SAN (Storage Area Network) and virtual servers has been installed at the Smith location which serves as the alternate processing facility. The set-up of the backups to replicate data will be completed over the summer.

BOCES provides internet through a router at the main District building through the District's internal firewall. Spectrum is the alternate internet provider if the BOCES internet fails. However, in the event of a server room failure occurring, the remaining District buildings will not have Internet access and therefore will not be able to access the business applications that are hosted at BOCES. The District Administration Team has evaluated the cost for establishing internet access for the other District Buildings and have found the cost to be prohibitive. It should be noted that the RIC also has a local McEvoy location which provides alternative workspace.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Business Continuity discussions have begun with RIC officials. To date, the District Business Office has developed plans for certain critical functions (such as payroll by having the ACH file to the bank a week ahead of time) to ensure timely functioning in the event that IT systems are not available. However, these plans do not cover all critical school functions. In addition, the District needs to continue to develop its Business Impact Analysis to identify critical business functions and the potential impact of an outage and develop measures to mitigate the impact.

Previous Years' Observation

Currently, with the exception of the phone system, the District does not have offsite disaster recovery capabilities to recover the network and systems that are hosted by the District in the event that the primary server room located at the High School is rendered inoperable. Plans are being established to locate the offsite disaster recovery to Smith Elementary School which will include a SAN to provide the necessary storage to recover from a failure. In the event that internet access was lost, District staff would relocate to BOCES to process payroll and financials. The District has not conducted a Business Impact Analysis (BIA) to determine the timeframes in which they can operate without having access to key instructional and district business applications and overall IT infrastructure services (e.g., internet access, access to email). In addition, the Business Impact Analysis would determine the amount of data that the District's departments and instructional areas are willing to lose in the event of an IT system failure. These results from the Business Impact Analysis would determine whether data backup strategies are designed to meet the District requirements and the extent in which an alternate location is needed to operate the District's IT systems in the event the primary server room was inoperable. Currently, there is not an alternate location that has been identified to operate the District's IT systems in the event the primary server room was inoperable. In the event that internet access was lost, District staff would relocate to BOCES to process payroll and financials.

Risk

Without a formal contingency plan that has been tested, there is risk that upon the loss or interruption of the IT function, data could be irretrievable and the School District's processing capability diminished.

Previous Years' Recommendation

1. We recommend the School District develop a Business Impact Analysis (BIA) which identifies Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all application systems and key IT services.
2. Based on the completion of the BIA, alternate processing locations should be established, a disaster recovery plan created and a process to test the plan.
3. The District needs to assess alternative network design solutions to enable the other District buildings to be able to connect to the proposed offsite disaster recovery site to allow for access to BOCES and the internet.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Payroll/HR-General Employee Administration

2016-02 *Segregation of Duties- Payroll/Human Resources*

Current Year Status:

The District has implemented the negotiations module within its accounting software which uses the set rates of pay by year of the applicable contract, and rolls each of them forward with the start of each new year. The District should continue to review its segregation issues around which department enters applicable pay rates and review of any rate changes throughout the year. The District did implement stronger mitigating controls surrounding the certification of payroll process whereby a change report is reviewed and analyzed each payroll cycle which shows all changes made between payroll runs. The District has elected to *tolerate* the remaining risks related to segregation of duties in this area. No corrective action is necessary.

Prior Year Observation

It was noted that the payroll department enters employee salaries and rates of pay. Segregation of duties could be strengthened by having the human resource department enter the employee's salary into the nVision system. In addition new salaries and pay rates are not properly reviewed and recalculated prior to the new fiscal year.

Prior Year Recommendation

Currently, the human resource department is meeting with the District's new employees and going over required documentation. This documentation is contained within a checklist form and ensures that the District has all required documentation for employees. In addition, when employees are hired they are given a proposed salary amount that is calculated by administration prior to being hired. In order to properly segregate payroll controls, human resource department should enter the new employee's salary into the financial software. Payroll should simply be entering the employee's payroll related deductions.

We also recommend that before the start of each fiscal year the human resource department review all upcoming increases in pay rates and salaries and enter them into the financial software. These rates would be recalculated and traced to supporting documentation such as contracts or agreements with employees. The payroll department should then review and recalculate the pay rates and salaries entered by the human resource department as a second check. This would also ensure that individuals whom have attained a longevity status would have the proper longevity paid. The human resource department would be best for this step as they have control over the personnel files and all pertinent information for each employee. We also recommend that after the recalculation of new salaries and rates, performance of this control be documented by initialing or signing a report showing the rates.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Payroll/HR-General Employee Administration

2016-03 *Exit Interview Checklist*

Current Year Status:

Upon an employee leaving the District, a letter informing them of their rights to an exit conference as well as information regarding health insurance is sent out. This meeting is not mandatory and the employee chooses whether they wish to attend or not. The District currently does not have an approved exit conference checklist. In addition, the District has not implemented the recommendation regarding Human Resource and the insurance function. This is still being handled by the payroll office. The District treasurer reviews all health insurance bills for accuracy on a monthly basis.

Prior Year Observation

We noted that the District does not have a proper exit conference with employees leaving the service of the District. We also noted with regards to health insurance that the human resource department does not handle the add, drops, or changes in coverage. This process is currently being done by the payroll department.

Prior Year Recommendation

When employees leave the District due to retirement, resignation, or termination; the District does not hold a proper exit conference, nor have they implemented a checklist of all needed documentation items. We recommend that the District develop an exit conference checklist for the human resource department to complete when an employee leaves the District. This checklist should contain information regarding any retirement planning, health insurance including COBRA coverage, and payment for retirement or insurance. In addition, this checklist will ensure that any employee leaving the District is properly informed of any benefits that are legally applicable to them. It will also serve as notice that employees are no longer employed with the District, thus eliminating the possibility of non-employees receiving district employee benefits.

We also recommend that the human resource department take control of the District's health insurance process. The human resource department is best suited to administer the health insurance process as they deal with employees on a more personal level. The human resource department should also be monitoring the health insurance bill to ensure that any non-district employees are removed from the insurance roster. Pertaining to the exit conference checklist the human resource department would be the first to know of any employee leaving the District, and therefore could change the eligible health insurance coverage for exiting employees. Also any changes in coverage should be done by the human resource department as they are in control of the employee's personnel files, which is where all change documents should be properly kept.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Special Aid-Compliance

2017-02 *Uniform Guidance Procurement Policies*

Current Year Status:

The District has updated its procurement policy in accordance with Uniform Guidance. The documentation of procurement procedures over compliance in accordance with Uniform Guidance is in process. The District should also develop risk assessments and internal control structure listings regarding each of their federal grants received. These documents should include all compliance objectives per grant and show how the District will respond to specific compliance objectives; as well as the controls in place to ensure compliance with each objective. These should be reviewed and updated annually as needed.

Prior Year Observation

On December 26, 2014 the Office of Management and Budget's Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, more commonly referred to as the "Uniform Guidance," became effective for all Federal awards, whether the funds are provided directly from a Federal agency or passed-through another state or local agency. The District currently has effective procedural controls in place over the management of Federal awards as concluded through the testing of grant expenditures. However, key changes under the Uniform Guidance expanded the rules regarding the documentation of internal controls over Federal Awards to require that they be documented in writing in the District's policies and that management should evaluate and document the results of ongoing monitoring to identify internal control issues. The written internal controls should specifically address each of the twelve (12) compliance requirements of the Federal Award Programs.

The Uniform Guidance has allowed a two (2) fiscal year implementation period from the date Uniform Guidance came into effect. This deferment of implementation should be done through Board resolution per the guidance through June 30, 2017. **Updated:** ***As of May 17, 2017 the OMB has granted an additional year for implementation of this policy.***

Prior Year Risk

The District will not be in compliance with Federal Grant regulations

Prior Year Recommendation

The District should document policies and procedures in accordance with the new Uniform Guidance. The new procurement policies and procedures should be in place for the June 30, 2019 fiscal year grants.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Information Technology – Network Security

2017-03 *Computer Security*

Current Year Status:

The District has set all computers to retrieve and apply Windows patches when they are made available. A beta version of Windows Server Update Services (WSUS) server has been implemented for this purpose. This version does not include the robust version of reporting that will enable personnel to monitor the success of monthly patching efforts. The District intends to research patching compliance reporting mechanisms, install a suitable product, and use this reporting to monitor the success of monthly patching.

Prior Year's Status

The District has set all computers to retrieve and apply Windows patches when they are made available. However, this approach does not provide a mechanism for determining whether these patches have been successfully applied to all endpoints. We recommend that the District install an SCCM server to deploy security patches and agents installed on all endpoints to allow the District to monitor the implementation status of security patches deployed to all endpoints and reapply patches which were not deployed.

The District has deployed Aristotle software on all District managed endpoints which provide content filtering and protects these endpoints from BOT viruses when they are on and off the District's network.

Prior Year Observation

The District has deployed Deep Freeze on all of its computers except for the laptops used by the administrative staff. Deep Freeze is a product used to allow the District to wipe out any changes made to a computer by restoring the previous day's image each day. The approach of using Deep Freeze was based on the understanding that District would be protected if a computer was infiltrated or attacked by malware. However, Deep Freeze will not prevent a vulnerability from being exploited which is due to the District not applying the monthly Microsoft security patches.

When District users surf the internet from inside the District network, reputation filtering of these visited sites is performed by a web proxy. For the few District laptops that have been issued to the administrative staff, when these laptops are taken outside of the District, reputation filtering of websites visited will not occur.

Risk

Computers used throughout the district will be subject to exploitation of security vulnerabilities.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Laptops used outside of the District will be subject to BOT attacks.

Previous Years' Recommendations

Establish a security patching program which applies security patches at least on a quarterly basis.

As part of the new Aruba Wi-Fi network, devices will be used with the administrative staff's laptops which will be set-up to not work on public Wi-Fi and only allow a secure connection to the District's internal network.

Information Technology – Network Security

2017-04 *Security of IT Service Accounts*

Current Year Status:

The District is the process of implementing two factor authentications for remote access. Windows logs are being collected and an effective review process is being performed.

Prior Year's Status

The number of users permitted remote access to the district's internal network via VPN has increased especially with the current work at home requirements. Currently, the District permits 15 individuals (i.e., comprised of IT staff, Business office, the Superintendent and direct reports) to remotely access the District's internal network. User remote access requires Windows Activity Directory security authentication. However, with the increased number of cyber-attacks throughout the education industry, it is recommended that the District evaluate the feasibility of implementing two-factor authentication for all remote access into the District.

Previous Years' Observation

IT installations make use of service accounts to run automated, scheduled background tasks for various purposes, including system maintenance, backups, administrative tasks, and other important processes. The account is afforded the access necessary to perform these tasks, and it is often extensive and sometimes all encompassing.

These accounts are typically reserved for automated, non-interactive use to run background tasks and are not intended for individual use during interactive sessions. We observed that these accounts are not restricted from interactive logon and use.

Risk

Since these accounts need to be set-up to not lock, an attacker could use a brute-force attack to take over these accounts.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Previous Years' Recommendation

Set up service accounts to prevent interactive logon.

The District has limited system processing occurring within the District internal domain. The District currently only utilizes two service accounts to run these systems. In order to reduce the disruption caused by these accounts if an attacker was able to gain control of them, the District should investigate the feasibility of configuring these service accounts to prevent interactive logons.

Information Technology – Financial Application Security

2017-05 *Security Access Provisioning and Recertification – nVision Application*

Current Year Status:

A new Business Official has been hired to replace the previous one and has both nVision and School District experience. This person has begun evaluating the role structure and has made some cursory changes to the existing roles already in place. nVision's software vendor is releasing enhancements in the next several weeks which are expected to improve security reporting. Using this new information, the Business Official plans to conduct a more in-depth review of the entire functional security design and the members assigned to those access roles. Any needed changes will be implemented, and records of the review will be retained for future inspection.

Prior Year's Status

During a school restructuring effort completed over the past year, access (including both functions and scope as determined by building code access) was reviewed by the Business Official as part of this effort. The functional access review was limited due to the limitations in functional access reporting which would aid in this effort. An effective process is in place to track and maintain evidence of all nVision security access changes that are made.

We recommend that the District continue its efforts with the nVision provider to enhance the reporting to make this effort less cumbersome. An annual review should be performed to ensure both functional access and scope levels remain appropriate. Reporting should enable a reviewer to, at a minimum, select sensitive functions and identify who is assigned these capabilities.

We recommend, going forward, recertifying (1) user access to the roles as assigned, and (2) the building and department codes assigned to each individual user, as users may move from building to building. Results of recertifications and any required adjustments should be retained.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Previous Years' Observation

The District's processes include the assignment of user security entitlements to application systems based on an individual's job requirements. The access is generally assigned either through predefined security roles or customizing the access of users with unique access requirements based on their individual job function.

The provisioning process for *nVision* involves an email to the Business Administrator from the user's manager in the form of a free form text based email, detailing the access required for a new user, or the change required for a specific individual to perform specific tasks, either based

on new job requirements or due to an inability to access specific functions or data. Predefined roles have not been established to enable a uniform, simple access setup. To complete the provisioning process the Business Administrator sends the request to BOCES to apply the security changes.

Based on compliance testing performed during the audit individual users were granted access that extends beyond the requirements of their job function. In addition, there were BOCES personnel which had privilege access that extends beyond their security administration function.

Most hiring and/or transfers take place within the summer recess period. During this time, access to the application is reviewed. However, this review is limited to whether the user is still an active employee, and does not extend to a full review of access privileges to determine whether they remain appropriate and commensurate with the user's access requirements.

It is an industry best practice to perform a recertification of user access on a periodic basis, and for it to include the details of the user's access. The District needs to enhance the process.

Risk

There is no assurance that District users are assigned the appropriate level of access. Transferring employees may also retain their access from previous responsibilities.

Previous Years' Recommendation

1. For each job category, establish a series of roles and determine the associated access requirements for each one. Distribute it to users and create an access request form containing the roles for the requestors to choose from when making a formal request.

2. Enhance the recertification process to include a detailed review of each user's access privileges

PRIOR YEAR RISKS AND RECOMMENDATIONS

Information Technology - Network Security

2018-02 Network Security Monitoring

Current Year Status

BOCES provides to The District three distinct reports from the Cisco firewall on a weekly monthly basis:

- **FW Advanced Malware Report**
- **FW Attacks Risk Report**
- **FW Network Risk Report**

These reports contain a significant amount of information regarding various network events which have occurred. The District has not established a formal process to track investigations initiated from the reviews that the District performs.

Prior Year's Status

BOCES has acknowledged during the risk assessment that they have some responsibility for monitoring network security activity. BOCES has represented that they have established global level security reports which they review, and email security alerts configured which they take action on. BOCES has acknowledged that the tools being used are being further enhanced to improve the monitoring which includes deploying a SIEM. BOCES has recently made network security reports available to the District which will form the basis for their network security monitoring. The District has also implemented Crowdstrike Falcon Advanced Threat Protection, which monitors logons and tracks for abnormal activity. Reports are generated daily for review by the IT team to identify suspicious activity. The District has sufficiently *treated* the risk related to this observation.

Previous Years' Observation

BOCES provides Internet access for the District in which District traffic is routed through an edge router and a District firewall which is managed and configured by *BOCES*. A service agreement does not exist between the District and *BOCES* which defines the network security monitoring responsibilities of *BOCES*. Based on the IT Director's discussions with *BOCES* during the audit, *BOCES* indicated they do not perform any network security monitoring on behalf of the District.

Risk

Cyber-attacks attempting to access District resources would not be detected.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Previous Years' Recommendation

The District should request that BOCES establish a log server to route the Firewall logs and the District should establish an internal network security monitoring function.

Extraclassroom - General

2018-03 *Faculty Auditor*

Current Year Status

The District has established an annual review of the extraclassroom binders that reflect the policies and procedures based on the recommendations of NYS Finance Pamphlet 2. The District is also dividing the accounts between the junior high and senior high as well as working with the booster club to assist with the sports related activities that are not currently being ran as a bonafide Extraclassroom activity. The District is also working on an annual training that will be required for all advisors. The District is in the process of addressing this recommendation.

Prior Year Observation:

We noted that while the District does have Extraclassroom policies and procedures contained within their policies, they could be strengthened. Although the Board adopted a policy governing the operations of the Extraclassroom funds, it did not ensure that District officials implemented and enforced said policy. The Extraclassroom policy dictates that a faculty auditor be appointed and subsequently lists the duties of said position. However, this position was not filled or appointed at the time of testing. We also noted that the procedures listed for the Central Treasurer are not being followed or completed, which was noted through observation and inquiry.

Prior Year Recommendation:

The Board should review their Extraclassroom policy and revise the current procedures to reflect the current policy. The Board should appoint a faculty auditor to perform the duties listed in the current policy.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Extraclassroom -Cash and Cash Receipts

2018-04 *Cash Receipts*

Current Year Status

The District has established an annual review of the extraclassroom binders that reflect the policies and procedures based on the recommendations of NYS Finance Pamphlet 2. The District is also dividing the accounts between the junior high and senior high as well as working with the booster club to assist with the sports related activities that are not currently being ran as a bonafide Extraclassroom activity. The District is also working on an annual training that will be required for all advisors. The District is in the process of addressing this recommendation.

Prior Year Observation:

In the previous years report during our testing of Extraclassroom receipts, we noted various discrepancies with the receipts from no backup documentation to substantiate the amount of the receipt to elongated amounts of time deposit took to be received at the District's banking institution. We also noted issues with the Central Treasurer signing off on receipts as the club treasurer and that Sales Tax was not being remitted as New York State Sales Tax guide dictates.

Prior Year Recommendation:

We recommend the Board appoint a faculty auditor as stated within their current policy, and task them with at least annual procedures where they review all cash receipts and disbursements for completion with respect to current board policies and procedures. The faculty auditor should also prepare a report for the Board at least bi-annually to ensure compliance with the set policies and procedures over the Extraclassroom fund.

Extraclassroom - General

2018-05 *Extraclassroom Club Folders*

Current Year Status:

The District has established an annual review of the extraclassroom binders that reflect the policies and procedures based on the recommendations of NYS Finance Pamphlet 2. The District is also dividing the accounts between the junior high and senior high as well as working with the booster club to assist with the sports related activities that are not currently being ran as a bonafide Extraclassroom activity. The District is also working on an annual training that will be required for all advisors. The District is in the process of addressing this recommendation.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Prior Year Observation:

For the previous year's audit, we attempted to review the club produced binders. The District had recently implemented the policy and procedure for each club to maintain a binder. We noted that many of them were not complete with respect to having the proper forms and documentation related to club activities contained within them.

Prior Year Recommendation:

Since this is a new procedure put in place by the District, we recommend that once the Board has appointed a faculty auditor, this person should review these club folders during their testing to ensure the club is maintaining copies of all receipts and disbursements, as well as maintaining their ledger to their current account balance. This also is a requirement of NYS Finance Pamphlet 2 in which there are two sets of records, one with the club and one with the Central Treasurer. It will also satisfy the requirement that student treasurers maintain their own ledgers.

Extraclassroom - General

2018-06 *Extraclassroom Clubs*

Current Year Status:

The District has established an annual review of the extraclassroom binders that reflect the policies and procedures based on the recommendations of NYS Finance Pamphlet 2. The District is also dividing the accounts between the junior high and senior high as well as working with the booster club to assist with the sports related activities that are not currently being ran as a bonafide Extraclassroom activity. The District is also working on an annual training that will be required for all advisors. The District is in the process of addressing this recommendation.

Prior Year Observation:

For the previous year's audit, we noted that some were not legitimate clubs that fit within the parameters of NYS Finance Pamphlet 2. These clubs consisted of a school store that had been closed for a number of years, principal's holding account for the high school and middle school, as well as a holding account for an after-prom party.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Prior Year Recommendation:

We recommend the district revaluate all clubs currently holding a balance and determine the validity of the club upon reviewing the club parameters within NYS Finance Pamphet 2. In essence, all clubs need to be for a defined purpose, with an approved club charter, approved by the Board, and have elected officers.

Information Technology - General Controls

2019-01 *Security Awareness*

Current Year Status:

The IT Department has developed 3 security awareness training modules in the form of PowerPoint Presentations color coded as Yellow, Orange, and Red for levels of advancement of subject matter. These include advisories and content in a wide variety of security topics, from protecting one's account/password, to social media behavior, phishing, malware and other security related threats, to laws and regulations on information privacy and District policies on information security. These PowerPoints were distributed through BOCES but is planned to be managed by the District during the next school year which will allow for effective tracking to ensure all required personnel completed the training.

Prior Year's Status

Presently, the IT department sends out weekly email cybersecurity bulletins. In the 3rd quarter of 2020, cybersecurity will be included in formal training for the entire District Staff.

Previous Years' Observation

School Districts and their service providers have increasingly become targets for intruders. Automated security tools provide a certain level of protection against intruders, but a strong security program also requires user awareness to the increasingly sophisticated methods and techniques employed by hackers.

Risk

Lack of user awareness leaves any entity vulnerable to these techniques and the threats they pose.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Previous Years' Recommendation

Develop a security awareness presentation and present it to District users. Periodically review it for new threats that require greater user awareness and understanding. The IT Director plans to attend a presentation by DHS to assist in developing a program.

Cash Receipts/Billing - Medicaid

2019-02 Medicaid Cash Receipts and Billing Submissions

Current Year Status:

The District has been meeting with relevant staff and BOCES representatives to ensure the District is taking full advantage of the services being offered as well as following up with relevant staff to ensure specific compliance. The District also receives reports from BOCES showing all rejected claims, and following up on these claims to ensure reimbursement. The District has effectively *treated* this risk.

Prior Year Observation

We noted through inquiry that the District relies on BOCES for their Medicaid claims submissions. BOCES will pull reports from the system and submit for reimbursement. Once this occurs the District will receive a statement stating the amount of claims submitted and the dollar amount of the reimbursement. In addition, the report will show the amount of claims rejected. The backup behind the claim submissions and rejections was not being sent to the District on a regular basis as of our inquiry.

Prior Year Risk

Claims could have been rejected for simple reasons that could be easily fixed by the District but without the backup, the District will be unaware of the claims rejected and reasons behind the rejections on a timely basis.

Prior Year Recommendation

The District should review this data periodically to ensure that all services that could be billed are being billed and that all claims that have been rejected have been followed up on and resubmitted if possible.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Information Technology-Governance

2020-01 State Privacy Regulation Implementation

Current Year Status:

The District established a list of approved vendor software which forms the basis of all possible vendors which may be inscope for ED2 Part 121. In addition, the District has external legal counsel develop a standard contract amendment in which the District is using to obtain inscope vendor executed contract amendments. The District is working with BOCES templates to identify the level of NIST compliance and will proceed with the identification of gaps and remediation plans during the next school year. In addition, a vendor oversight program will be established using a Risk based approach.

Prior Year's Observation

Project initiatives were established at the District with objective of meeting all the requirements set forth to meet NYS ED Section 2D Regulation 121 (Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information).

The District has completed many of the required initiatives which include:

- Establishing a parents' bill of rights for data privacy and security which includes all the required 2D components that is posted on the District's website
- Breach reporting and compliant handling procedures
- Designating a Data Protection Officer (DPO)

The following project initiatives remain to be completed:

- Establish an inventory of PII data stored at the District and shared with 3rd parties
- Establish data security and privacy controls that are aligned with NIST CSF v 1.1

The District has contracted with BOCES to assist the District completing these two remaining initiatives.

Prior Year's Recommendation:

Proceed with plans to establish a complete PII inventory and establish a mechanism to identify NIST components that need to enhance data security and privacy controls.

PRIOR YEAR RISKS AND RECOMMENDATIONS

2020-02 Vendor Management – NutriKids

Current Year Status:

The District purchases cafeteria services through BOCES. At this time BOCES has not shared their future migration timelines of a new system migration with the new District. If the District migrates to Heartland's Mosaic system, it is understood that they are in the process of undergoing a SOC 2 review.

Prior Year's Observation

The District will migrate their Cafeteria services from the on-premise hosted NutriKids system to Heartland Solutions' Mosaic system, which is operated in the Cloud. As of this time, Heartland Solutions it is unclear whether they have undertaken an independent control evaluation of their environment (SOC 2).

Risk

The District will not identify control issues within the vendor's processing environment.

Prior Year's Recommendation

It is recommended that the District contact Heartland Solutions to determine whether they have undergone a SOC 2 review. If they have undergone the review, request the report and perform a review to assess whether it is acceptable to the District.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Information Technology – Application Security

2020-03 Application Logon Security - Transfinder

Current Year Status

A new cloud-based version of Transfinder is scheduled for implementation in the summer of 2021.

Prior Year's Observation

Logon security is achieved by establishing processes to prevent the unauthorized takeover of a user's ID. The controls used to prevent this occurrence are comprised of effective password construction controls, provisions to lock IDs after successive failed logon attempts and an overall monitoring process.

The following logon security issues were identified within the *Transfinder* application:

- Passwords are not a minimum of characters in length
- Passwords do not expire
- Accounts do not lock out for a period of time after repeated invalid logon attempts to prevent unlimited repeated attempts

Risk

Weak, unchanged passwords increase risk of a user ID being compromised.

Prior Year's Recommendation

It is understood that the Transfinder vendor will be releasing a system upgrade which will address these logon security issues. The District should install this upgrade once it is made available by the vendor.

RESULTS OF ANNUAL TESTWORK

EXECUTIVE SUMMARY – IT REVIEW

D'Arcangelo & Co., LLP was requested by the *Cortland School District* Board of Education and the Audit Committee to conduct procedures related to the District's Information Technology function. The following is a summary of the procedures performed and the outcome of those procedures.

Disaster Recovery

Disaster Recovery and Business Continuity Planning

Testwork Performed:

The audit procedures that we performed included the following:

- Validate that a Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) have been established for all district processes which are mapped to applications and IT services
- Determine whether RPO and RTOs are specified in service agreements for all critical school district systems hosted at third party locations
- Reviewed for completeness of the District's Disaster Recovery Plan
- Determine whether recovery capabilities exist in the event the internet services are disrupted at the server room
- Reviewed the Disaster Recovery Testing performed to ensure it evaluates the effectiveness of the Disaster Recovery Plan
- Validated that backup schedule is executed for District systems that are hosted on-premises.

Observation:

Development and evaluation of the Disaster Recovery Plan is being viewed from the standpoint of where business systems are hosted and the means of reaching them in the event of a primary site failure.

The District has an effective process for backing up their data to the alternate site at the Smith. In the event of site failure of the primary IT site at the high school the District has the ability to restore processing to maintain services that are hosted at the District at the Smith Building. However, Internet access is currently has not been established at the alternate site. Since all of the District business applications (i.e., with the exception of Food Service and transportation) are currently hosted at BOCES or vendor sites, there is limited processing that could be performed at the alternate site.

Validated that backup schedule is executed for District systems that are hosted on-premises.

EXECUTIVE SUMMARY – IT REVIEW

Recommendations:

1. Complete analysis and deploy Internet access from the Smith Building
2. Proceed with plans to test the disaster recovery site at the Smith Building. It should be noted that the generator is being tested weekly.
3. Update system inventories for application and infrastructure products in order to identify recovery requirements and establish priorities.
4. Update RTOs and RPOs with collaboration with District departments to ensure proper recovery planning by priority.

Governance

Data Classification, Data Retention and Data Privacy compliance

Testwork Performed:

The audit procedures that we performed included the following:

- Determine whether project initiatives have been completed to meet NYS ED Section 2D Regulation 121 (Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information) prior to the compliance date of July 1, 2020. Evaluate the progress made in the following components of ED 2D Part 121:'
    - Establish an inventory of PII data stored at the District and shared with 3rd parties
    - Establish a parents' bill of rights for data privacy and security which includes all of the required 2D components that is posted on the district's website
    - Determine whether the district has designated a Data Protection Officer (DPO)
    - Identifying vendors who receive district PII data
    - Tracking of vendors approached who have district PII data to sign contract amendments to be ED 2 compliant
    - Update district security and privacy standards based on NIST implementation and tracking of project initiatives to resolve all gaps
    - Establishing Breach reporting and complaint handling procedures which includes portal for parents to post

- The District has established data retention standards based on ED-1

- Determine whether a Data Classification standard has been established and implemented.
- Determine whether advanced security awareness training has occurred to ensure district personnel and students (i.e., if students have access to the district's internal domain) do not fall prey to a social engineering attack

EXECUTIVE SUMMARY – IT REVIEW

Observation:

The District has completed many of the required initiatives which include:

- Establishing a parents' bill of rights for data privacy and security which includes all the required 2D components that is posted on the District's website
- Breach reporting and complaint handling procedures
- Designating a Data Protection Officer (DPO)
- Establish an inventory of PII data stored at the District and shared with 3rd party vendors
- Executed contract amendments with most 3rd party vendors which have access to District's PII data

The following project initiatives remain to be completed:

The District established a list of approved vendor software which forms the basis of all possible vendors which may be inscope for ED2 Part 121. In addition, the District has external legal counsel develop a standard contract amendment in which the District is using to obtain inscope vendor executed contract amendments. The District is working with BOCES templates to identify the level of NIST compliance and will proceed with the identification of gaps and remediation plans during the next school year. In addition, a vendor oversight program will be established using a Risk based approach.

The project initiative that relates to implementing a data classification standard will be addressed as part of the alignment of the NIST framework to District Security and Privacy protocols.

The District partially completed the project to identify all PII data as required by ED 2-D Part 121 (Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information). Additional measures are required to have a complete list of vendors that are inscope for ED-2 Part 121.

The IT Department has developed 3 security awareness training modules in the form of PowerPoint Presentations color codes as Yellow, Orange, and Red for levels of advancement of subject matter. These include advisories and content in a wide variety of security topics, from protecting one's account/password, to social media behavior, phishing, malware and other security related threats, to laws and regulations on information privacy and District policies on information security. These PowerPoints were distributed through BOCES but is planned to be managed by the District during the next school year which will allow for effective tracking to ensure all required personnel completed the training.

EXECUTIVE SUMMARY – IT REVIEW

The District will be establishing a project initiative during the next school year to establish email phishing tests at the District. In addition, DLP solutions are being investigated to possibly deploy at the District. The District currently receives and reviews Google reports for possible instances of data leakage.

Recommendations:

1. Proceed with plans to establish a complete PII inventory and establish a mechanism to identify NIST components that require analysis to determine their current compliance state.
2. Complete the project to obtain remaining contract amendments from 3rd party vendors who are provided District PII data.
3. Establish a process to conduct oversight of 3rd party vendors who receive PII data to ensure they are meeting their security commitments.
4. Proceed with the project initiative to implement a data classification standard.
5. Proceed with the remaining ED-1 project initiatives.
6. Proceed with plans to roll out the 2021 version of the security awareness training program.
7. Proceed with plans to establish an email phishing test campaign.
8. Proceed with plans to investigate DLP solutions.

Application Security

School District Application Systems Access Controls

Testwork Performed:

School Tool application is used by the District to manage all student information as it relates to instruction and administrative areas. The system is hosted at BOCES but the authentication to access this system occurs through the On-premises Active Directory authentication. During this summer the District has established a project initiative to migrate this to google authentication which occurs in the cloud.

nVision is used by the District to manage its financials, issue vendor disbursement checks and to handle the employee payroll. The system is hosted at BOCES is accessible to the Internet.

The District is currently using NutriKids for their Cafeteria services which will be migrated in the near future by BOCES to a solution that is not hosted at the District.

The IEP Direct application is used by the District to manage all aspects of the Special Education program which is hosted by the vendor in the Cloud.

EXECUTIVE SUMMARY – IT REVIEW

Edulog is the transportation system used at the District and is hosted on-premises at the District.

The audit procedures that we performed included the following:

- Determine whether application security is set to lock an ID after successive invalid logon attempts
- Determine whether application password construction controls exist

Observation:

All District systems reviewed had adequate logon security control except for NutriKids and Edulog. NutriKids will be replaced with another system in the near future which is a project being managed by BOCES. Edulog will be rolled out to a cloud-based version which has enhanced logon security controls.

Recommendations:

Proceed with plans as guided by BOCES for the replacement of NutriKids
Proceed with plans to replace Transfinder with the cloud version of Transfinder (Routefinder Pro).

Network Security

Internal Domain Security

Testwork Performed:

The audit procedures that we performed included the following:

- Determine whether privileged account management solutions have been implemented at the District
- Determine whether effective domain logon security controls have been established
- Determine whether an effective process has been established to ensure that anti-virus is installed on all District workstations, laptops and servers and updated virus definitions and security patches are deployed on a timely basis.
- Determine whether an effective web proxy has been deployed that prevents district personnel from connecting to Internet sites which can initiate BOT and other malware attacks
- Determine whether windows domains logs are retained which supports an effective domain and host level security review.

EXECUTIVE SUMMARY – IT REVIEW

Observation:

The District has represented that Crowdstrike Falcon has been fully deployed on all desktops, laptops and Chromebooks. The District has replaced their traditional virus protection methods using Crowdstrike. Some capabilities which are available in Crowdstrike are currently being provided by other tools such as AristotleK12 and Lightspeed. All of these security tools were examined during this review, and when combined with Crowdstrike provide adequate coverage of the environment.

The District has not established a formal process to track investigations initiated from the reviews that the District performs as it relates to Crowdstrike, Aristotle, and Lightspeed alerts.

The District has set all computers to retrieve and apply Windows patches when they are made available. A beta version of Windows Server Update Services (WSUS) server has been implemented for this purpose. This version does not include the robust version of reporting that will enable personnel to monitor the success of monthly patching efforts. The District intends to research patching compliance reporting mechanisms, install a suitable product, and use this reporting to monitor the success of monthly patching.

Individual privileged domain accounts are properly assigned.

Account lockouts have been established at the network level for 5 consecutive invalid logon attempts, with a 10-minute lockout period. However, additional control measures are needed to reduce the risk of an unauthorized takeover of an ID.

Windows logs are being retained and are being properly reviewed.

Recommendations:

1. Establish formal process for tracking security incident investigations.
2. Proceed with plans to upgrade the District's security patch deployment analysis capabilities.

EXECUTIVE SUMMARY – IT REVIEW

Network Security

External Network Security

Testwork Performed:

The audit procedures that we performed included the following:

- Determine whether a firewall have been effectively deployed to prevent unauthorized internet-based connections
- Determine whether a log server has been established to capture network activity which supports an effective review process
- Determine whether the District is performing an effective review of firewall flagged events
- Determine whether the district conducts periodic network vulnerability scans
- Determine whether two-factor authentication has been implemented for all remote access into the District's internal domain.

Observation:

The District has not deployed two-factor authentication for remote access into the District's systems.

The District uses Google suite for email and google drives. The administrative accounts are not configured to require two factor authentications.

The District has not performed vulnerability scans of its external facing network. It is understood that the overall risk of the internal domain is not of a high risk since most District applications are not hosted at the District.

The Audit team ran licensed tools to assess the adequacy of firewall configuration security set-up. The results did identify some security deficiencies with the manner in which the firewall was configured.

EXECUTIVE SUMMARY – IT REVIEW

BOCES provides to The District three distinct reports from the Cisco firewall on a weekly monthly basis:

- FW Advanced Malware Report
- FW Attacks Risk Report
- FW Network Risk Report

These reports contain a significant amount of information regarding various network events which have occurred. The District has not established a formal process to track investigations initiated from the reviews that the District performs.

The District has deployed the advanced threat protection features that are available within its external firewall. These layer 7 capabilities include deep packet inspection and holistic threat analysis capabilities.

For all other test procedures, we found no other control design or effectiveness issues.

Recommendations:

1. Investigate the feasibility of implementing two-factor authentication to further secure the IT Staffs' and third-party service providers' privileged windows accounts. For third party service providers who refuse to support District using two factor authentications additional control measures will be pursued by the District.
2. Proceed with a cost/benefit analysis of licensing a vulnerability scanning tool to periodically test the external facing District IPs.
3. Establish two factor authentications to access the Google administrator account.
4. Establish a formal process to track investigation which arise from external network security activity.
5. Perform analysis of automated reports which identifies security vulnerabilities within the firewall rules and initiate remediation plans where possible.

ADDITIONAL TEST WORK PERFORMED

Payroll/HR-General Employee Administration

Targeted Employee Payroll Analysis

Objective

The objective of this analysis was to determine that key administrative employees with the most risk of management override were paid according to their contracted salary.

Procedures Performed and Outcome

We targeted six (6) high risk employees with access to the financial software or could have access to the financial software. We recalculated all payroll payments made to the employee for the period July 1, 2020 through May 31, 2021. We observed no instances where salary paid represented a gross deviation from the contracts set forth by the District contracts.

Recommendation

No recommendation necessary based on the outcome of procedures performed.

Payroll/HR-General Employee Administration

Targeted Employee Same as Vendor

Objective

The objective of this test was to look at any payments made to targeted employees outside of payroll, and ensure they appear reasonable. After any matches are found we investigate all payments made and look into anything that appears to be suspicious.

Procedures Performed and Outcome

We targeted six (6) high risk employees with access to the financial software or could have access to the financial software. We then scanned the entire disbursements journal for payments made to these individuals. All occurrences of payments made to these individuals were reviewed. The payments were made up of contractual payments as well as mileage reimbursements. All payments appeared reasonable.

Recommendations

No recommendation deemed necessary based on the outcome of procedures performed.

ADDITIONAL TEST WORK PERFORMED

Benford's Law Analysis

Objective

The objective of this analysis was to apply statistical reasoning to possibly identify potential issues contained in the disbursement journal.

Background

Benford's Law is a statistical anomaly that was first discovered by Simon Newcomb and then further analyzed by Frank Benford. This law states that the odds of a number appearing at any point within a number are predictable. For example, below is a chart containing the statistical odds of any given number being the first digit of a larger number.

Digit	1	2	3	4	5	6	7	8	9
Odds of Obtaining as 1st Digit (%)	30.1	17.6	12.5	9.7	7.9	6.7	5.8	5.1	4.6

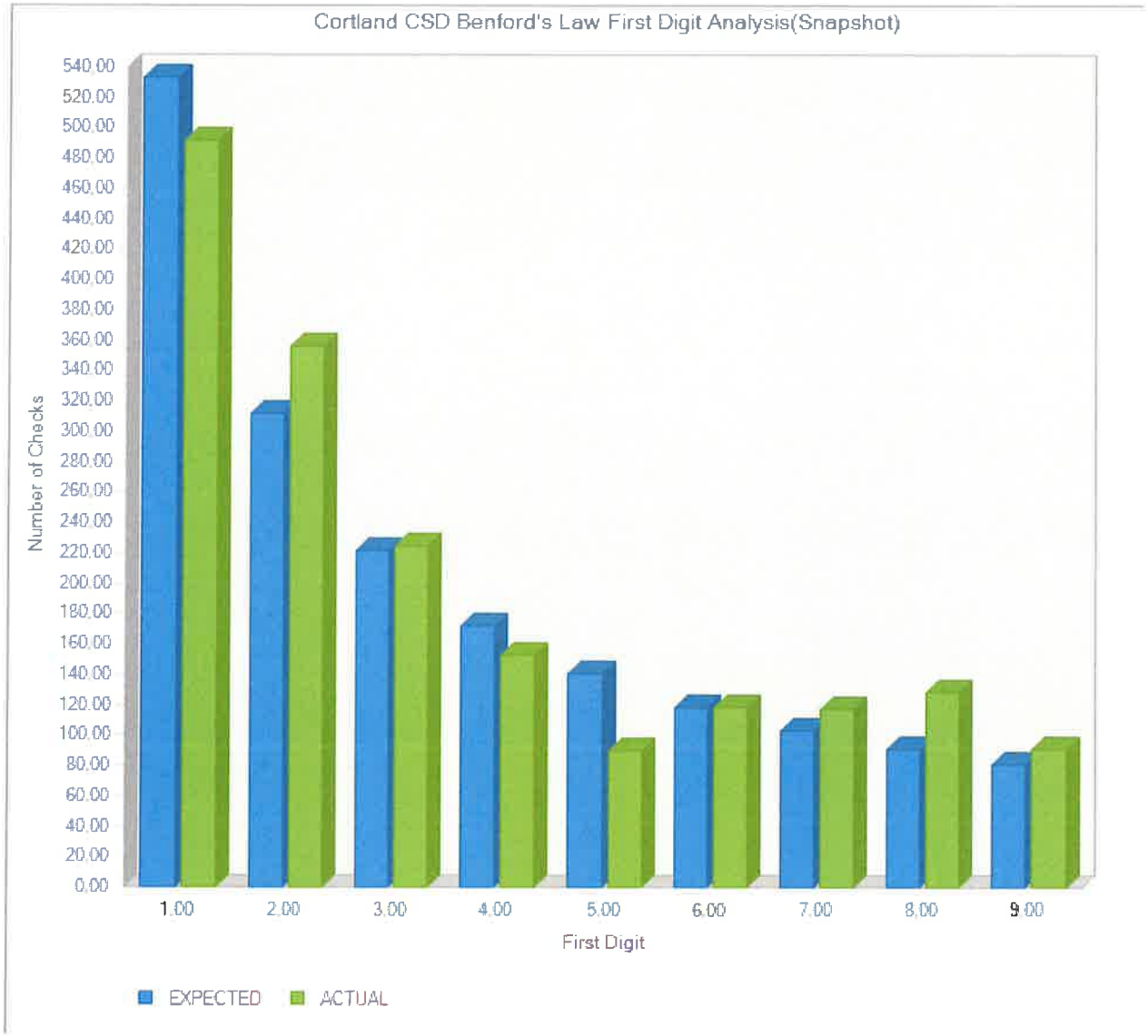
(http://intuitor.com/statistics/Benford's%20Law.html)

The odds of the number one being in the first position is 30.1%. By comparing a set of data to these criteria we could identify areas to look into further.

Procedures Performed and Outcome

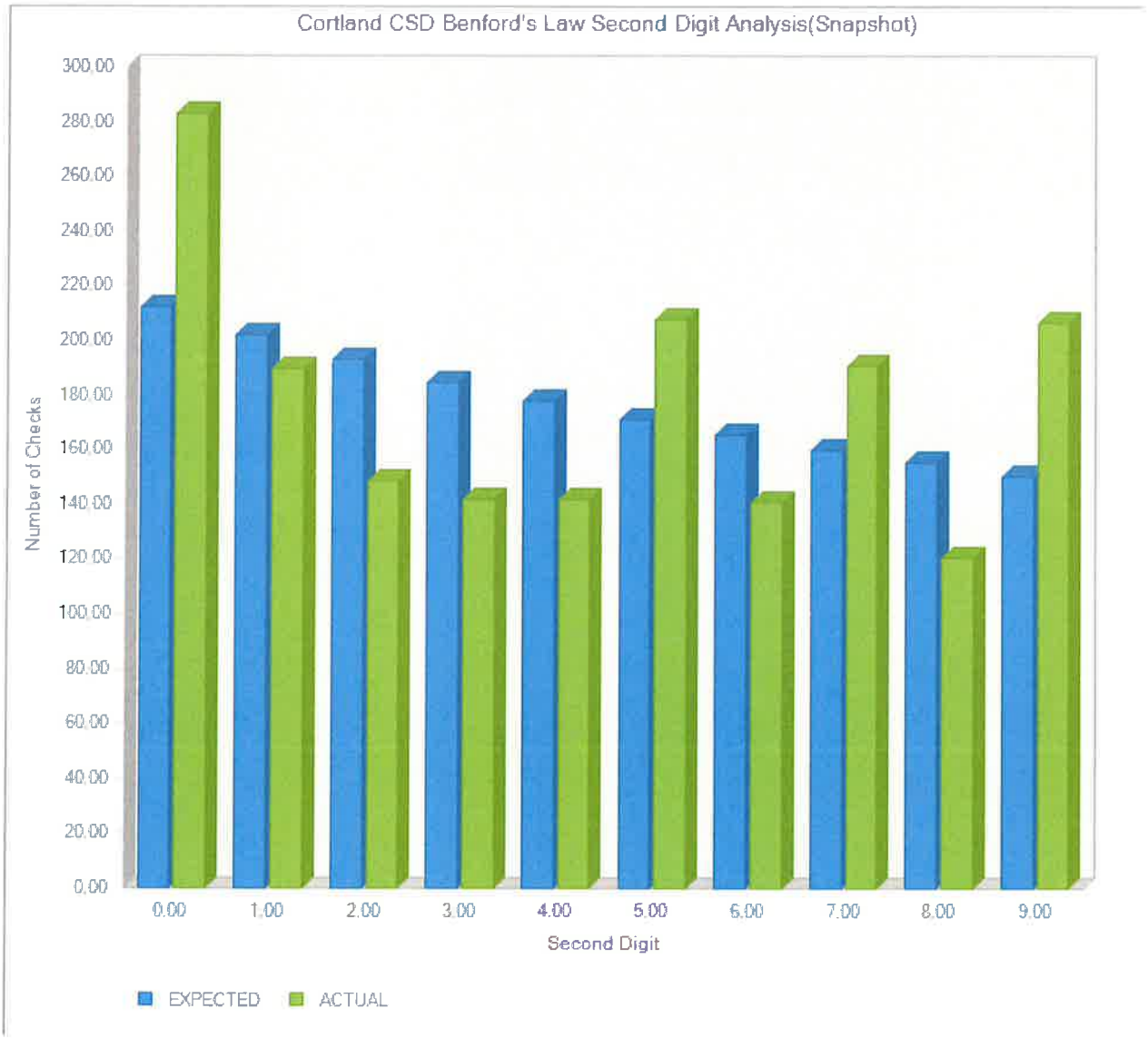
By applying Benford's Law to the District's disbursement journal data for the period of July 1, 2020 through May 31, 2021, the following results were calculated for both the first digit and second digit.

ADDITIONAL TEST WORK PERFORMED



Results for 1st Digit Test

The first digit Benford's Law Analysis showed abnormal variances against the expected counts for the first digits of 2, 7, 8, and 9. The majority of the variances for the first digit of 2, 7, and 8 were for payments to athletic officials for refereeing and athletic event management. The first digit of 8 was also represented by recurring payments made to contracted vendors. The first digit of 9 variance was represented by payroll deduction payments for employee selected deductions.



Results for 2nd Digit Test

In performing the second digit Benford's law Analysis we saw an abnormally higher than expected number of check amounts with the second digit of "0, 5, 7, and 9". The second digit 0 can be explained by a large number of even dollar checks for contractual and self-insurance payments. For example, 100, 200, 500, 1,000. The second digit of 5 and 7 variance was represented by payments made to individuals athletic event management such as referee. The second digit of 9 variance was represented by payroll payments for insurance and other employee payroll related deductions.

ADDITIONAL TEST WORK PERFORMED

Duplicate Payment and Gap Detection Test:

Objective

To ensure that all payments made by the District were only made once, and that there was a logical sequence of checks issued. In addition, any check gaps could be adequately explained and not due to fraud, error, or omission.

Procedures Performed

We obtained a check register for all funds for the time period of July 1, 2020 through May 31, 2021. From this listing, we extracted all payments made to the same vendor for the same amount. From this sample, we tested potential duplicates using professional judgment to ensure they were for legitimate purchases or claims and not duplicate payments. We noted no duplicate payments made during the time period tested.

We also utilized this check list to run a gap detection test, which pinpoints any gaps in the logical sequence of check numbers. From this report, we reviewed all gaps in the sequence to ensure they were for legitimate reasons, such as voids or system limitations. We noted that all check gaps were for system limitations and reasonable.

Recommendations

No recommendation deemed necessary based on the outcome of procedures performed.