CORTLAND ENLARGED
CITY SCHOOL DISTRICT

INTERNAL AUDIT

RISK ASSESSMENT UPDATE
AND
ANNUAL TESTWORK

July 19, 2022

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 update to the initial risk assessment and annual test work for the year ended June 30, 2022 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 the standards required by the Regulations of the Commissioner of Education.

The engagement to perform the update to the 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 19, 2022

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 19, 2022

Risk Assessment Update

Business Unit	Process	Inherent Risk				Control Risk				Testwork Performed					
		As of July 19, 2022													
		Severe	High	Mod	Low	Severe	High	Mod	Low	2018	2019	2020	2021	2022	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 19, 2022

Business Unit	Process	Risk Assessment Update								Testwork Performed					
		Inherent Risk				Control Risk									
		As of July 19, 2022													
		Severe	High	Mod	Low	Severe	High	Mod	Low	2018	2019	2020	2021	2022	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		✓					✓						✓	Pages 28 - 29
	Payments Outside P.O. System	✓						✓						✓	Pages 28 - 29
	Procurement Process	✓					✓							✓	Pages 28 - 29
	Private Purpose Trust Expenditures			✓				✓							
	Reporting Requirements		✓					✓						✓	Pages 28 - 29
	Allocation of Expenditures	✓						✓						✓	Pages 28 - 29
	Payment Processing	✓						✓						✓	Pages 28 - 29
	Petty Cash Administration			✓				✓							
State Aid	General Processing/Monitoring		✓					✓							
	Basic Aid		✓					✓							
	Transportation Aid			✓				✓							
	Building Aid/Capital		✓					✓							
	Excess Cost Aid			✓				✓			✓				
	BCCES			✓				✓							

RISK REGISTER AS OF July 19, 2022

		Risk Assessment Update													
Business Unit	Process	Inherent Risk				Control Risk				Testwork Performed					
		As of July 19, 2022													
		Severe	High	Mod	Low	Severe	High	Mod	Low	2018	2019	2020	2021	2022	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 19, 2022

		Risk Assessment Update													
Business Unit	Process	Inherent Risk				Control Risk				Testwork Performed					
		As of July 19, 2022													
		Severe	High	Mod	Low	Severe	High	Mod	Low	2018	2019	2020	2021	2022	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

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.

- 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.

2015-04 *Data Classification*

Current Year Status

The ED 2 initiative has taken a lower priority during this Pandemic period. This will be a higher priority to complete during upcoming year as part of the NIST CSF implementation project required by ED-2.

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

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 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 RISKS AND RECOMMENDATIONS

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

Current Year Status

The records management officer retired this past year. As of July, 2021 a new records management officer and records access officer has been appointed. This initiative will be addressed during this upcoming year which will include establishing the District's interpretation of ED-1 data retention requirements and implement the required storage solutions.

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

2015-06 *Contingency Plan*

Current Year Status

With the migration of transportation system to the vendor's cloud-based environment, the District does not host any District business applications on premises. Backup and recovery services have been established at the Smith building. Individual Internet devices have been purchased to allow for limited Internet access throughout the District in the event of a disruption to the District's primary Internet connection. The Business Impact Analysis should still be completed for all critical District applications to ensure the service provider which hosts these systems are meeting the District's recovery objectives.

Previous Years' 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. 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.

PRIOR YEAR RISKS AND RECOMMENDATIONS

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. Proceed with plans to establish cost effective solutions to establish alternative Internet connectivity for District buildings in the event that District's Internet connection is disrupted.
2. Proceed with plans to establish backup processes to the Smith School.
3. Proceed with plans to establish a Business impact Analysis to ensure recovery requirements are being met.
4. Establish testing to support recovery requirements.

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.

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.

PRIOR YEAR RISKS AND RECOMMENDATIONS

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.

2017-03 *Computer Security*

Current Year Status

The District has established reporting to provide a mechanism to monitor the effectiveness of its security patching program.

Previous Years' Observation

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.

Risk

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

Previous Years' Recommendations

Proceed with plans to deploy reporting to monitor the effectiveness of the security patching program.

PRIOR YEAR RISKS AND RECOMMENDATIONS

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

Current Year Status

A new business official has been hired since the last review who is responsible for access provisioning and the recertification process. An evaluation of the role structure will occur which will support any adjustments to the security design which will be used to support an effective recertification process.

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. It is industry best practice to perform an annual recertification that individuals are assigned the proper access based on the requirements of their job function. Past efforts to perform an effective recertification process were limited due to the lack of reports that are provided by nVision.

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

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

2018-01 *Vendor Management*

Current Year Status

BOCES recently completed a SSAE 18 service SOC 2 Type 2 audit in which BOCES established a restricted process in order for School Districts to have the opportunity to review this report. The District should request access to this report from CNYRIC to ensure the services they use were included in the scope of the audit and all existing exceptions identified in the report presented no risk to the District.

Previous Years' 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

PRIOR YEAR RISKS AND RECOMMENDATIONS

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.

CNYRIC has indicated that a recent SOC audit was completed of the CNYRIC service organization. The District should request a copy of this report to ensure there are no issues identified that present a risk to the District,

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.

Prior Year's Recommendation

The District should request a copy of this report to ensure there are no issues identified that present a risk to the District,

PRIOR YEAR RISKS AND RECOMMENDATIONS

2018-02 Network Security Monitoring

Current Year Status

Based on the frequent status meetings that have been established within the IT team and the limited number of incidents that require follow-up investigations there are no additional measures that need to be taken. No corrective action needed.

Previous Years' Observation

BOCES has acknowledged 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 provides the District three Distinct network security reports to support the District's network security review process. 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 not established a formal process to track investigations initiated from the reviews that the District performs.

Risk

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

Previous Years' Recommendation

Establish a process to identify issues from the security reviews which require follow-up investigations.

PRIOR YEAR RISKS AND RECOMMENDATIONS

2018-03 *Extraclassroom-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.

2018-04 *Extraclassroom- 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 RISKS AND RECOMMENDATIONS

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.

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 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 RISKS AND RECOMMENDATIONS

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.

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 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.

PRIOR YEAR RISKS AND RECOMMENDATIONS

2019-01 *Security Awareness*

Current Year Status

All District staff were required to complete security awareness training which included tracking of participation. The establishment of an email phishing test program will be evaluated during the next year. It should be noted that the security awareness training materials were updated to include email phishing to train staff on the different attack methods which are used.

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.

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.

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.

The District plans to deploy an initiative to perform an email phishing test of its staff to ensure that it does not fall prey to social engineering attacks.

Risk

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

Previous Years' Recommendation

Proceed with planned initiatives.

PRIOR YEAR RISKS AND RECOMMENDATIONS

2020-01 *Remote VPN Access*

Current Year Status

The District has reduced the number of individuals who granted the ability to remote into the Districts' network to only IT personnel. The District no longer hosts any of the key District business applications and has limited use of shared drives with the usage of Google Docs. The District is evaluating other solution providers to meet this security control.

Previous Years' Observation

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.

Risk

Unauthorized takeover of privileged administrator accounts could occur.

Previous Years' Recommendation

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.

2020-03 Application Logon Security - Transfinder

Current Year Status

The District migrated to the cloud-based version of Transfinder. However, the system has a deficient logon security issue in which there is not a minimum number of characters in a password. The District should follow up with the vendor to determine whether this is a control feature they will consider establishing in the future.

Transfinder did not undertake a SOC 2 audit of their environment. With Transfinder being hosted where it is accessible from the Internet, not having an independent audit performed such as a SOC review presents significant risk to the District. The District

PRIOR YEAR RISKS AND RECOMMENDATIONS

should contact the vendor to indicate their concerns that an independent oversight review such as a SOC 2 has not been performed of their environment.

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

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

Risk

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

Prior Year's Recommendation

Proceed with plans to migrate to the new cloud-based version of Transfinder.

2020-04 State Privacy Regulation Implementation

Current Year Status

The District established a portal to track the contract disposition of all its inscope ED-2 Vendors. Most of the software inscope for ED-2 are purchased through the BOCES in which BOCES has the contract relationship. BOCES established portal accessible to all Districts which provides a copy of all the vendor contracts in which it manages the contract relationship. Currently, the District is in the final stages of validating the BOCES portal to ensure that it addresses all the vendors they contract through BOCES.

PRIOR YEAR RISKS AND RECOMMENDATIONS

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 following is the status of the District's progress in addressing the remaining open items required to meet ED2 requirements:

- 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.
- The District had 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.
- A vendor oversight program will be established using a Risk based approach.

Prior Year's Recommendation:

Proceed with planned initiatives to address the remaining open items required to meet ED2 requirements.

CURRENT RISKS AND RECOMMENDATIONS

Information Technology - Governance

2022-01 Vendor Management

Observation

The District uses IEPDirect which is hosted at Frontline. IEP Direct is a web-based application that is accessible from the internet. The District has not reviewed the latest SOC 2 report issued by Frontline (testing period: June 1 2020 to May 31 2021) to ensure the services they use were included in the scope of the audit and all existing exceptions identified in the report presented no risk to the District. The District did not maintain any documentation for audit of this review, or the specific procedures followed.

Risk

The District's review of the SOC 2 report may not be sufficient to properly identify risks to the District.

Recommendation

The District should request the latest SOC 2 report from Frontline and perform their review of the report to ensure there is not any risk which impacts the District. The District should formalize its process for review of all SOC 2 reports through the use of a checklist that will document the review and ensure all risks to the District are properly identified and communicated.

CURRENT YEAR RISK AND RECOMMENDATIONS

2022-02 Acceptable Use of Technology Resources

Observation

An acceptable use policy (AUP) was developed that addresses both staff and student use. The policy does contain provisions for use of email and issued laptops for personal use, but does not address cloud technology such as google docs, meeting software, etc.

The staff and student acceptance of the (AUP) is typically based on obtaining digital signatures or annual completion of AUP forms to confirm reading, understanding, and agreeing to abide by the policy. During the review, the District updated the Classlink and Windows access logon screens to display the acknowledge of acceptance of the AUP prior to login. The District plans to have District staff sign the AUP during the annual training sessions.

Risks

The current policy does not provide guidance and restrictions over newer technologies.

Any updated policy may not be acknowledged by staff members, both with this and future revisions.

Recommendation

Update the Acceptable Use Policies to govern the use of cloud based technologies.

RESULTS OF ANNUAL TESTWORK

EXECUTIVE SUMMARY

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 Purchasing and Accounts Payable function. We performed an internal audit of the Purchasing and Accounts Payable functions and related internal controls. Our internal audit was conducted to assess the level of compliance with procedures set forth by the District's Administration. We reviewed and evaluated the policies and practices relating to the District's purchasing and accounts payable functions. As part of this assessment, we interviewed selected staff, performed tests on selected purchase orders, receiving documentation and expense reports as deemed necessary to understand the process and to determine compliance.

Procedures Performed

As part of the annual testing we obtained the check registers for all funds for the time period of July 1, 2021 through April 1, 2022. We randomly selected One Hundred Fifty (150) disbursements for testing.

We performed the following procedures to ensure compliance with district policies and procedures:

- Verify voucher was obtained and utilized for purchase.
- Verify purchase has an applicable purchase order, verify amount, vendor, dates and addresses.
- Verify invoice is applicable for purchase. Recalculate invoice total for verification.
- Verify invoice amount agrees with purchase order amount.
- Ensure internal claims auditor approval on the invoice.
- Verify bidding purchases are following the procurement and purchasing policy set forth by the School district and Municipal Law Section 104-b.
- Verify the account code agrees from the voucher to the invoice. Verify purchase is in the correct account code. (Example- payroll is not recorded in supplies)
- Verify the dates of the invoice/purchase date are following the date of the PO.
- Verify the receiving PO is signed off for goods received.
- If packing slip was applicable verify the receiving employee signed off for goods received.
- Verify original purchase order is reviewed and approved by the purchasing agent before purchase.
- For athletic events, obtain the applicable claims form. Verify approval for claim appears reasonable.
- If purchase is for a capital project, verify capital project to the Board minutes for approval of project/vendor for applicable work performed.
- If disbursement is for a reimbursement, verify reimbursement form is used and approved.

EXECUTIVE SUMMARY

- Verify disbursement was included in the Warrant that the internal claim's auditor reviews and approves.
- Verify the Warrant was signed and that checks issued were in sequential order.

Outcome of Procedures Performed

Of the 150 cash disbursements, we reviewed for the time period of July 1, 2021 through April 1, 2022, totaling $1,591,043, we noted the following:

- Four (4) voucher packets contained invoices that were not initialed or signed as approved by the Claims Auditor.
- Ten (10) voucher packets were missing a signature by the district that the item purchased had been received.
- Open Purchase orders did not contain documentation of amounts paid on the original purchase order in order for the claims auditor to ensure the open purchase order was not overspent .
- Two (2) mileage claim forms were missing the district form for standard mileage reimbursements between buildings.
- One (1) voucher packet was for amount over the purchase order amount, with no indication of the purchase order being raised to cover the additional expenses.
- Four (4) voucher packets contained purchase orders over the competitive bid threshold, but no indication on the quotes that bids were solicited.
- Two (2) voucher packets were for services rendered by one individual. This payment did not contain a contractor type contract therefore could be viewed as an employee of the district by IRS regulations.
- Items purchased off of BOCES bids were not indicated on the purchase order as such to assist claims auditor.
- Claims auditor is not requesting/seeing bids or contracts in conjunction with their review as noted through inquiry of district personnel.

Recommendations:

We recommend that the district review their purchasing policies and bidding policies first to ensure they are up to date and in line with current practices. The district should ensure that bid / quote compliance is properly referenced in the voucher packet or on the purchase order. The claims auditor should on a periodic basis review the documentation referenced in the packet to ensure proper compliance with the districts procurement policy. In addition, the district should include in the voucher packet for any open purchase order the total amounts paid on the open purchase order. This will assist the claims auditor to ensure money is available on the open purchase order when purchases are made.

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, 2021 through April 1, 2022. 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

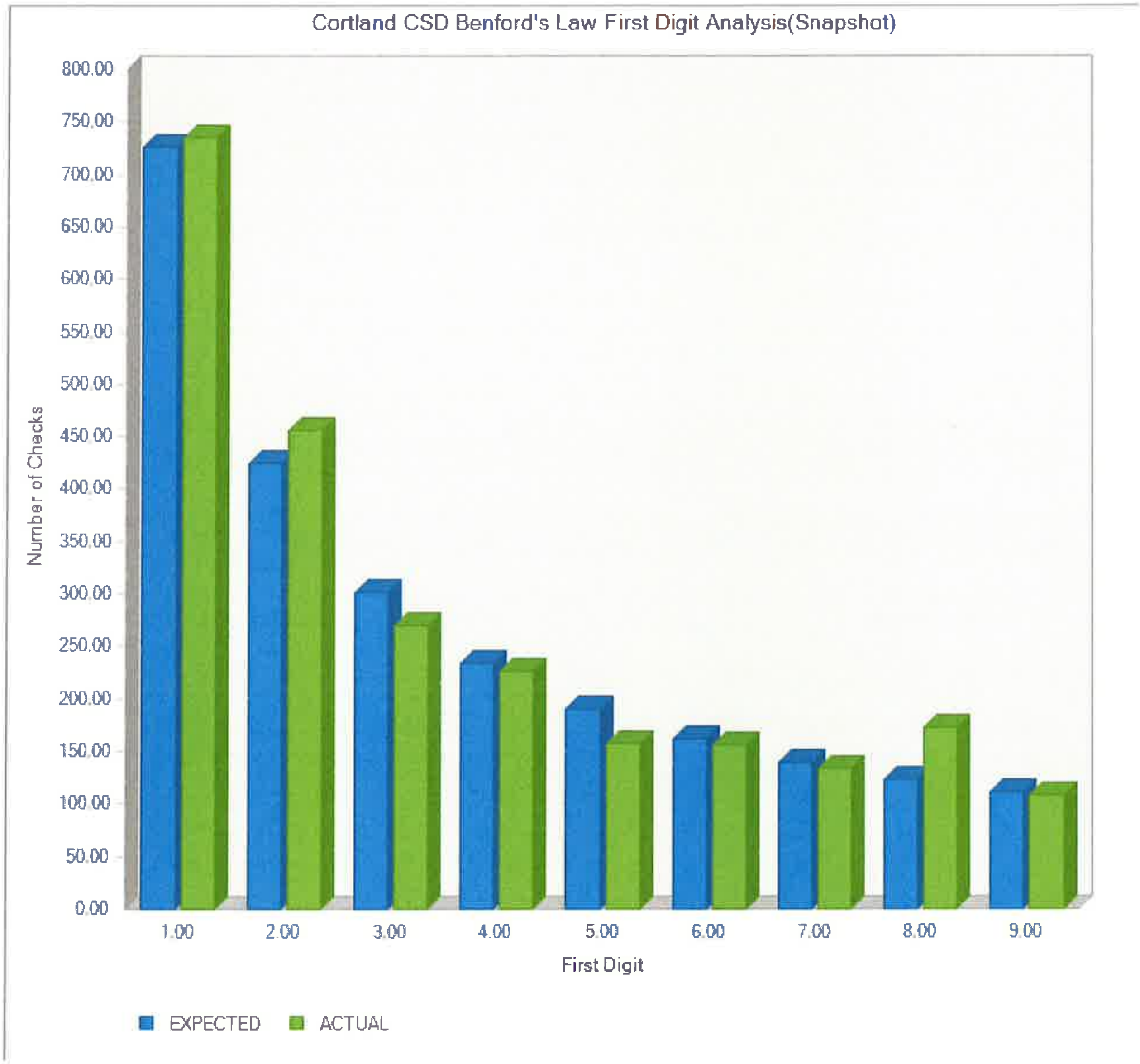
(http://intuitor.com/statistics/Benford's%20Law.html)

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, 2021 through April 1, 2022, the following results were calculated for both the first digit and second digit.

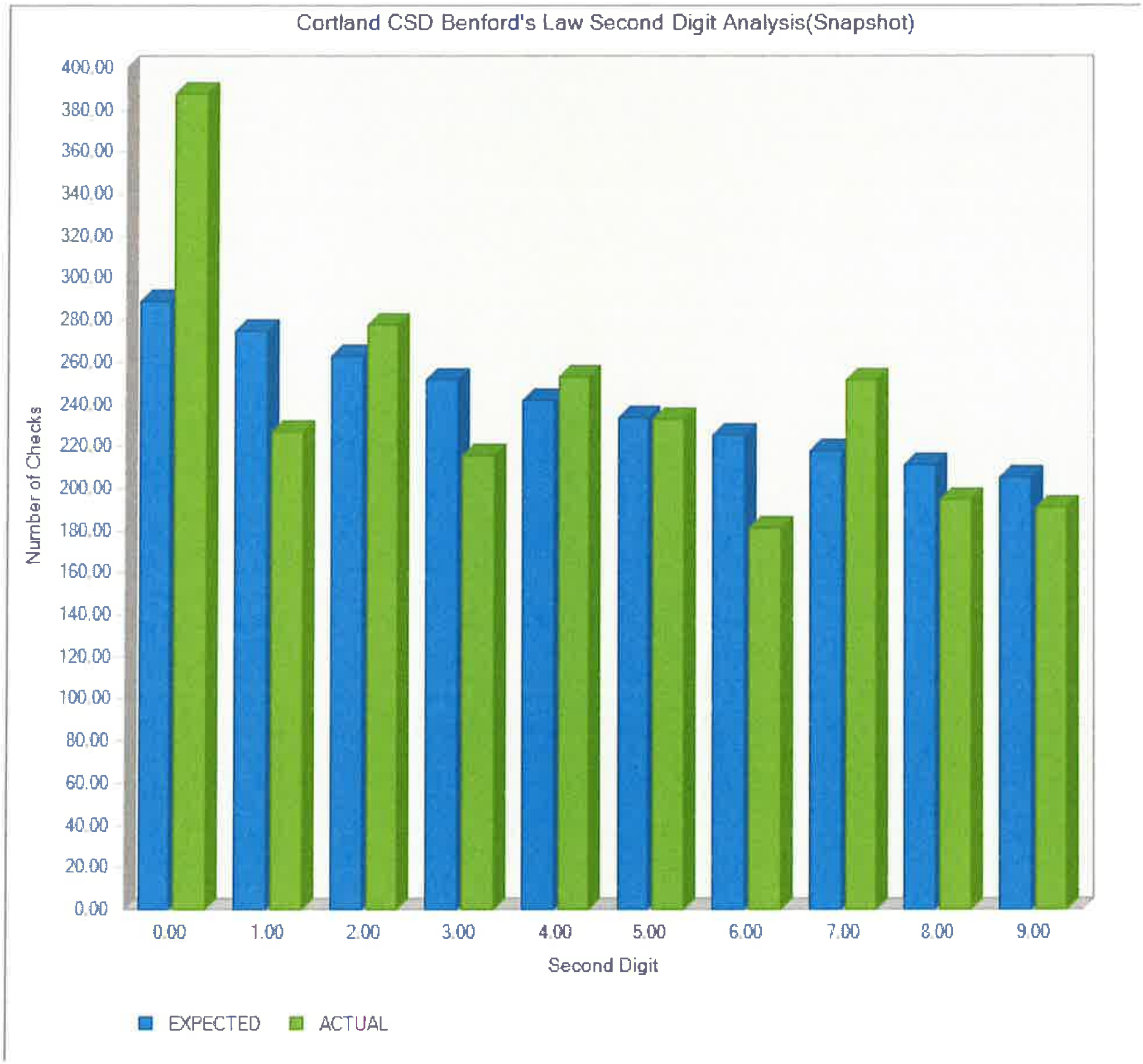
ADDITIONAL TEST WORK PERFORMED



<u>Results for 1st Digit Test</u>

The first digit Benford's Law Analysis showed abnormal variances against the expected counts for the first digits of 1, 2, and 8. The majority of the variances for the first digit of 1, 2, 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.

ADDITIONAL TEST WORK PERFORMED



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, 2, 4, and 7". 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.

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, 2021 through April 1, 2022. 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.