CORTLAND ENLARGED
CITY SCHOOL DISTRICT

INTERNAL AUDIT

RISK ASSESSMENT UPDATE
AND
ANNUAL TESTWORK

April 27, 2017

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 the Cortland Enlarged City School District in performing an initial risk assessment and annual test work for the year ended June 30, 2017 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 the Cortland Enlarged City School District and are the overall responsibility of the School District.

This report is intended solely for the 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

April 27, 2017

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 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 have 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 that are 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 April 27, 2017

		Risk Assessment Update											
Business Unit	Process	Inherent Risk				Control Risk				Testwork Performed			
		As of April 27, 2017											
		Severe	High	Mod	Low	Severe	High	Mod	Low	2015	2016	2017	Reference
Governance	General Policy and Procedures	✓					✓						
	Monitoring	✓						✓					
	Organizational Structure	✓						✓					
	Risk Management	✓						✓					
Information Technology (IT)	Governance/Security		✓				✓					✓	
	Financial Application 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 April 27, 2017

		Risk Assessment Update											
Business Unit	Process	Inherent Risk				Control Risk				Testwork Performed			
		As of April 27, 2017											
		Severe	High	Mod	Low	Severe	High	Mod	Low	2015	2016	2017	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 April 27, 2017

Business Unit	Process	Risk Assessment Update											
		Inherent Risk				Control Risk				Testwork Performed			
		As of April 27, 2017											
		Severe	High	Mod	Low	Severe	High	Mod	Low	2015	2016	2017	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 April 27, 2017

Business Unit	Process	Risk Assessment Update Inherent Risk As of April 27, 2017				Control Risk				Testwork Performed			
		Severe	High	Mod	Low	Severe	High	Mod	Low	2015	2016	2017	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

In order to assist the School District in managing its risks efficiently and effectively, we have summarized certain risks based on our professional judgment. For each of the risk areas highlighted, we have included a recommendation for the School District to consider in addressing the specific risk.

Governance-General Policy and Procedures

Inherent Risk- *Severe*
Control Risk- *High*
Risk Appetite- *Moderate*

Accounting Procedures Manual

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.

PRIOR YEAR RISKS AND RECOMMENDATIONS

- 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.

Current Year Status:

The District is in agreement with this recommendation and is continuing the process of documenting the processes in all relevant areas.

Governance-General Policy and Procedures

Inherent Risk- *Severe*
Control Risk- *High*
Risk Appetite- *Moderate*

Conflict of Interest Statements

Prior Year Observation

Currently neither the Board of Education nor management is required to sign an annual conflict of interest statement. Although not required by law, a conflict of interest statement is considered a best practice for purposes of transparency. The conflict of interest statement would disclose any relationship, contract, or transaction that could have an appearance of conflict with board members or key employee's decision.

Prior Year Risk

The District, unknowingly, could have a contractual relationship that could be deemed a conflict of interest for either a board member or key employee.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Prior Year Recommendation

We recommend the District require an annual conflict of interest statement be documented from its board members and key employees to disclose any potential appearance of a conflict of interest.

Current Year Status:

The district has contracted with Erie 1 BOCES to develop a conflict of interest policy and procedures part of an overall board policy update.

Governance-General Policy and Procedures

Inherent Risk- *Severe*
Control Risk- *High*
Risk Appetite- *Moderate*

Procurement Policy

Prior Year Observation

GML 104(b) requires that the District adopt a written procurement policy with procedures governing procurement of goods and services that are not subject to competitive bidding requirements. The policy and its procedures must provide for the use of written or verbal or other competitive procurement methods, procedures for determining which procurement method to use, circumstances when the solicitation of proposals or quotes will be waived, and the documentation standards for each method of procurement. In addition, it is important that a procurement policy address and provide guidance for emergency purchases, sole source purchases, and procurement of professional services and the documentation needed to support all purchasing decisions.

We noted that the district has updated this policy through Erie 1 BOCES, however the new version does not define the thresholds needed for compliance with General Municipal Law 104(b).

Prior Year Recommendation

The Board should review and update the District's procurement policy to ensure that it is in compliance with GML 104(b). The policy should include detailed and clear guidance on the documentation required for proof of compliance. Documentation may include memoranda, written quotation forms, telephone logs (for verbal quotes), RFPs, and copies of Federal, State, county contracts or other government contracts for which "piggybacking" is permitted. If a contract is awarded to an offer other than the lowest dollar offer, the policy must require that there be justification and documentation, setting forth the reasons the award.

Current Year Status:

The District is currently working with Erie 1 BOCES to revise all policies. This policy when revised should be reviewed to ensure it contains the necessary language associated with GLM 104(b).

Governance-General Policy and Procedures

Inherent Risk- *Severe*
Control Risk- *High*
Risk Appetite- *Moderate*

Internal Claims Auditor Procedures

Prior Year Observation

We noted though our audit that there is no policy in place pertaining to the claims auditor function. In addition there are no documented procedures or list of items that the board has determined the claims auditor to review prior to approving payments for purchases.

We also noted through inquiry that the claims auditor is not reviewing contract or bidding documentation for purchases to determine compliance with applicable laws.

Prior Year Recommendation

We recommend the board develop a checklist of procedures to be performed on all claims. The procedures should include review of documentation necessary for compliance with applicable laws, including but not limited to General Municipal Law 103 and 104(b).

Current Year Status:

The District utilizes outside contractor for internal claims audit services. The district should monitor the actions of this claims auditor and ensure they are following district polices as set forth by the Board of Education as well as utilizing a checklist for items reviewed during the claims audit process. Also on an annual basis claims auditor should meet in person with the board to go over at least a summary of annual findings.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Information Technology - Governance/Security

Inherent Risk – *High*
Control Risk – *High*
Risk Appetite – *Moderate*

Policies/Data Protection

Prior Year Observation

The District does not have an Acceptable use policy for Cloud-based offerings used for instructional and student/teacher collaboration. In addition, evaluations of cloud-based offerings have not been performed to ensure that controls are available to ensure that personal, private, and sensitive information are not be posted or stored within these Cloud-based offerings.

Prior Year Risk

- The New York State Comptroller states that comprehensive IT security policies and procedures should be in place to protect personal, private, and sensitive information (PPSI) and on mobile computing devices, including laptops, smartphones, tablets and portable media devices. As cloud based solutions are used by teachers and students in the District, there is the risk of sensitive and private information being uploaded to the cloud where it is not protected.

- Without an "Information Security Breach and Notification" policy #8635, identified as the policy legally required for all school districts, the District will not be in compliance with New York State law. School districts must disclose any breach of data to affected New York residents.

Prior Year Recommendation

1. Develop and adopt the "Use of and Access to Personal, Private, and Sensitive Information" policy. Define PPSI; explain the reasons for collecting PPSI; and describe specific procedures for the use, access to, storage, and disposal of PPSI involved in normal school activities. Staff should acknowledge that they have read, accept and understand the policy.

PRIOR YEAR RISKS AND RECOMMENDATIONS

2. Evaluate all Cloud-based offerings used by the District and assess whether sufficient security provisioning (i.e., setting up users which are permitted access), audit trails and content monitoring controls have been established.

Prior Year Status

The District currently has not deployed cloud based offerings but is planning to initiate this technology in the near future. The District will establish an initiative to cover the items included in the prior year's recommendation.

Current Year Status

Cloud based offerings have not been offered as of this time (Office 365). Therefore, the need to establish policies at this time as not required.

Information Technology – Governance/Security

Inherent Risk - *High*
Control Risk – *High*
Risk Appetite - *Moderate*

Vendor Management

Prior 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. 16 (SSAE 16) and Attestation Standards Section 101 (AT Section 101) in order to provide visibility within these service providers' control design. The SSAE 16 replaced the SAS 70 report on June 15, 2011.

PRIOR YEAR RISKS AND RECOMMENDATIONS

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* (*Central NY RIC)* 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 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.

Current Year Status

The District is the process of reviewing the BOCES SSAE 16 service auditor's assurance audit report and will have the Superintendent raise any issues to BOCES if there are any issues.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Information Technology – Governance/Security

Inherent Risk - *High*
Control Risk - *High*
Risk Appetite - *Moderate*

Data Classification

Prior Year 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.

Prior Year 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.

Current Year Status

The District plans to allocate time during the next year to complete the data classification project.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Information Technology-Disaster Recovery

Inherent Risk - *Severe*
Control Risk - *High*
Risk Appetite - *Moderate*

Contingency Plan

Updated Observation

Currently, with the exception of the Phone system, the District currently does not have offsite disaster recovery capabilities to recover the network and systems that are hosted by the district in the event that the High School is rendered inoperable. Plans are being established to locate the offsite disaster recovery site at the 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.

Prior Year 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.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Prior Year 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.

Current Year Status and Updated Recommendations

The district is in the middle of creating a Disaster Recovery plan to ensure power, phone, network connectivity to internet and data servers are available if the Core Switch at the JSHS was to become available. The Smith Elementary School has been designated as the disaster Recovery location. 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.

Information Technology- Security

Inherent Risk - *Severe*
Control Risk - *High*
Risk Appetite - *Moderate*

Network Security Monitoring

Prior Year Observation

BOCES provide 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.

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

Prior Year 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.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Current Year Status

As part of the District planned deployment of a new firewall with the District network, which will provide an additional layer of network security, the District will also implement their own network security monitoring.

Information Technology- Security

Inherent Risk - *High*
Control Risk - *High*
Risk Appetite - *Moderate*

Network Security

Prior Year Observation

The District's wireless network is established which provides connectivity to the District's internal network which uses WPA-2 security and require computers to have their MAC address defined to the a Radius Server. However, a wireless access point was established at the Kaufman for visitors to use which allows access to the District's internal network.

The District plans to establish a guest wireless network which has no access to the District's internal network as part of the network upgrade.

Prior Year Risk

Attacks can occur to resources which are not properly protected within the District's internal network.

Current Year Status

A guest wireless has been deployed. The district is also purchasing a new Aruba Wifi network which will include a guest wireless.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Information Technology- Security

Inherent Risk - *High*
Control Risk - *High*
Risk Appetite - *Moderate*

Network Security

Prior Year Observation

The District has IT services which are accessible from the internet which includes its email and the Student Information System, Infinite Campus. The District has not performed a network level vulnerability assessment to ensure that these internet accessible services do not have any critical vulnerabilities.

Prior Year Risk

Cyberattacks can occur to internet accessible IT resources.

Current Year Status

Since email is the only critical external facing service hosted at the district, the need to perform annual network vulnerability assessment is not as critical. During the Annual Testwork, the audit team utilized licensed vulnerability assessment tools to disclose 7 medium security risk vulnerabilities which the District plans to remediate.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Payroll/HR-General Employee Administration

Inherent Risk - *High*
Control Risk - *High*
Risk Appetite - *Moderate*

Segregation of Duties- Payroll/Human Resources

Prior Year Observation:

It was noted that the payroll department enters employee's salary 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 employees payroll related deductions.

We also recommend that before the start of each fiscal year that the human resource department review all upcoming increases in pay rates and salaries. 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 that performance of this control be documented by initialing or signing a report showing the rates.

Current Year Status:

There has been no change in district procedures and processes with regards to this comment. The district should review their process and update to include the above recommendation to mitigate any potential risks of deviations or incorrect data.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Payroll/HR-General Employee Administration

Inherent Risk - *High*
Control Risk - *High*
Risk Appetite - *Moderate*

Exit Interview Checklist

Prior Year Observation:

We noted that the district does not have a proper exit conference with employee's 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 appropriated 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 personnel 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, 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

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.

Payroll/HR Payments to Employees

Inherent Risk - *High*
Control Risk - *High*
Risk Appetite - *Moderate*

Certification of Payroll

Prior Year Observation:

We noted that the district's payroll system has an override function for paycheck amounts. This allows the individual processing payroll to override the set payroll amount each paycheck. An override report is not currently being produced for review by the individual certifying the payroll. We also noted the certification of payroll could be strengthened.

Prior Year Recommendation:

The district has implemented controls where a change report is produced prior to each payroll run that denotes any change in pay amounts between the current payroll and the prior payroll run.

Payroll certification could be strengthened by the individual certifying the payroll by randomly selecting 3 to 5% of employees each payroll and tracing their pay rates back to their agreed to salary amount or pay rate. This would ensure employees are being properly paid in accordance with their salary notice or contract rate. These individuals tested should be documented to prepare an effective audit trail.

Current Year Status:

The district has not implemented the change in procedure whereby randomly selected employees are being traced back to their salary notice to ensure be paid properly. The district has implemented the change in policy where a payroll change/comparison report is reviewed by management outside of the payroll process to ensure any changes out of the ordinary are reviewed and followed up on.

CURRENT YEAR RISKS AND RECOMMENDATIONS

Special Aid-Compliance

Inherent Risk - *High*
Control Risk - *High*
Risk Appetite - *Moderate*

Uniform Guidance Procurement Policies

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.***

Risk:

The District will not be in compliance with Federal Grant regulations

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.

RESULTS OF ANNUAL TESTWORK

ANNUAL TEST WORK OBSERVATIONS AND RECOMMENDATIONS

D'Arcangelo & Co., LLP was requested by the *Cortland Enlarged City School District* Board of Education and the Audit Committee to conduct procedures related to the Information Technology function as required in accordance with Chapter 263 of the laws of New York State for annual test work. The following are the observations and recommendations based on the test work performed:

Information Technology – Application Security

Inherent Risk – *High*
Control Risk – *High*
Risk Appetite – *Moderate*

Security Access Provisioning and Recertification – nVision Application

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 Official 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 Official 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.

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.

Information Technology – Application Security

Inherent Risk – *High*
Control Risk – *High*
Risk Appetite – *Moderate*

Security Access Provisioning and Recertification – IEP Direct Application

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 *IEP Direct* involves an email to the CSE Chair 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 were initially established to enable a uniform, simple access setup. However, compliance testing based on a sample review conducted with the CSE Chair disclosed that the limited number of roles used required individual users access privileges which are not required for their job function.

Additionally, there are outside entities and providers, such as preschools and head start programs, whose access is administered by BOCES. The Cortland CSE Chair was informed that reviews of access administered by BOCES is performed by BOCES, but she does not receive copies of the reviews performed and is unsure of the frequency and level of detail of the review.

ANNUAL TEST WORK OBSERVATIONS AND RECOMMENDATIONS

The Cortland CSE Chair performs an access review annually, but the review thus far has been limited to whether users listed remain within their positions, and did not include 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.

Risk

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

Outdated roles increase the probability of users being assigned access beyond what is required for their job responsibilities.

Recommendation

1. Prepare a list of job categories and identify the access needs for each. Perform a thorough review of each user within the roles and identify any instances where roles provide excessive access. Identify instances in which new roles need to be created and reassign users to the new roles as necessary. Document each role and create an access request form containing the roles for 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. Instruct BOCES to do the same and request copies of their reviews performed.

Information Technology – Application Security

Inherent Risk – *High*
Control Risk – *High*
Risk Appetite – *Moderate*

Application Logon Security - NutriKids

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.

ANNUAL TEST WORK OBSERVATIONS AND RECOMMENDATIONS

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

- Audit trails of security changes are not present in the system
- Passwords are hard coded by BOCES in the system and consist of the last 4 digits of each user's personal phone number, which makes them subject to easy compromise
- 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

The District will not identify attempts to access application systems, and weak, unchanged passwords increase risk of a user ID being compromised.

Recommendation

Request that the vendor implement the ability of the District to set logon and password controls in the system, including password length, complexity, expiration, and account lockout. Also, implement an audit trail to record all security related changes.

Information Technology – IT Governance

Inherent Risk – *High*
Control Risk – *High*
Risk Appetite – *Moderate*

Records Retention of Student and Business Records

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.

ANNUAL TEST WORK OBSERVATIONS AND RECOMMENDATIONS

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.

Information Technology – Network Security

Inherent Risk – *High*
Control Risk – *High*
Risk Appetite – *Moderate*

Network Security Design

Observation

The District Internet access is through the BOCES Syracuse Regional Information Center which is also used by all of the other Districts who use their services. BOCES has a firewall which permits District designated external connections to BOCES hosted District systems and systems that the District hosts within its internal network. The District does not have a firewall to prevent other school districts inside the BOCES network from attempting to access District internal IPs. In addition, district requires a firewall to secure the services hosted at the District because based on the review of the BOCES firewall rules during the audit it was identified that granular firewall rules have not been established ensure that only the required ports and services have been opened to access District hosted services.

The District does not perform periodic vulnerability assessments of its District hosted email which is reachable from the internet. During the audit, the audit team ran a licensed vulnerability assessment tools against the Lotus Notes server hosted which disclosed seven (7) medium risk security vulnerabilities.

Risk

The District will not be protected against other District attacks or attacks from the Internet.

Recommendations

Proceed as planned to install a firewall behind the District edge router.

Remediate the seven medium risk vulnerabilities identified on the Lotus Notes server.

ANNUAL TEST WORK OBSERVATIONS AND RECOMMENDATIONS

Information Technology – Network Security

Inherent Risk – *High*
Control Risk – *High*
Risk Appetite – *Moderate*

Security of IT Service Accounts

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 and attacker could use a brute-force attack to take over these accounts.

Recommendation

Set up service accounts to prevent interactive logon.

Information Technology – Network Security

Inherent Risk – *High*
Control Risk – *High*
Risk Appetite – *Moderate*

Computer Security

Observation

The District has deployed Deep Freeze on all of its computers except for the laptops used by the Administration 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 Administration staff, when these laptops are taken outside of the District, reputation filtering of websites visited will not occur.

Risk

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

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

Recommendations

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

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

Information Technology – Disaster Recovery

Inherent Risk – *High*
Control Risk – *High*
Risk Appetite – *Moderate*

Offsite Data Backup

The district performs offsite data backups of district data and email to the SAN located at the Barry Elementary school which is performed manually by a member of the IT staff. Offsite backups should occur on a daily basis and should be an automated process.

Risk

The District will potential lose data from the last 5 business days.

Recommendation
Establish an automated scheduled process to perform an offsite backup of district data on a daily basis.

ADDITIONAL TESTWORK 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 February 1, 2016 through December 1, 2016. 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 TESTWORK 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

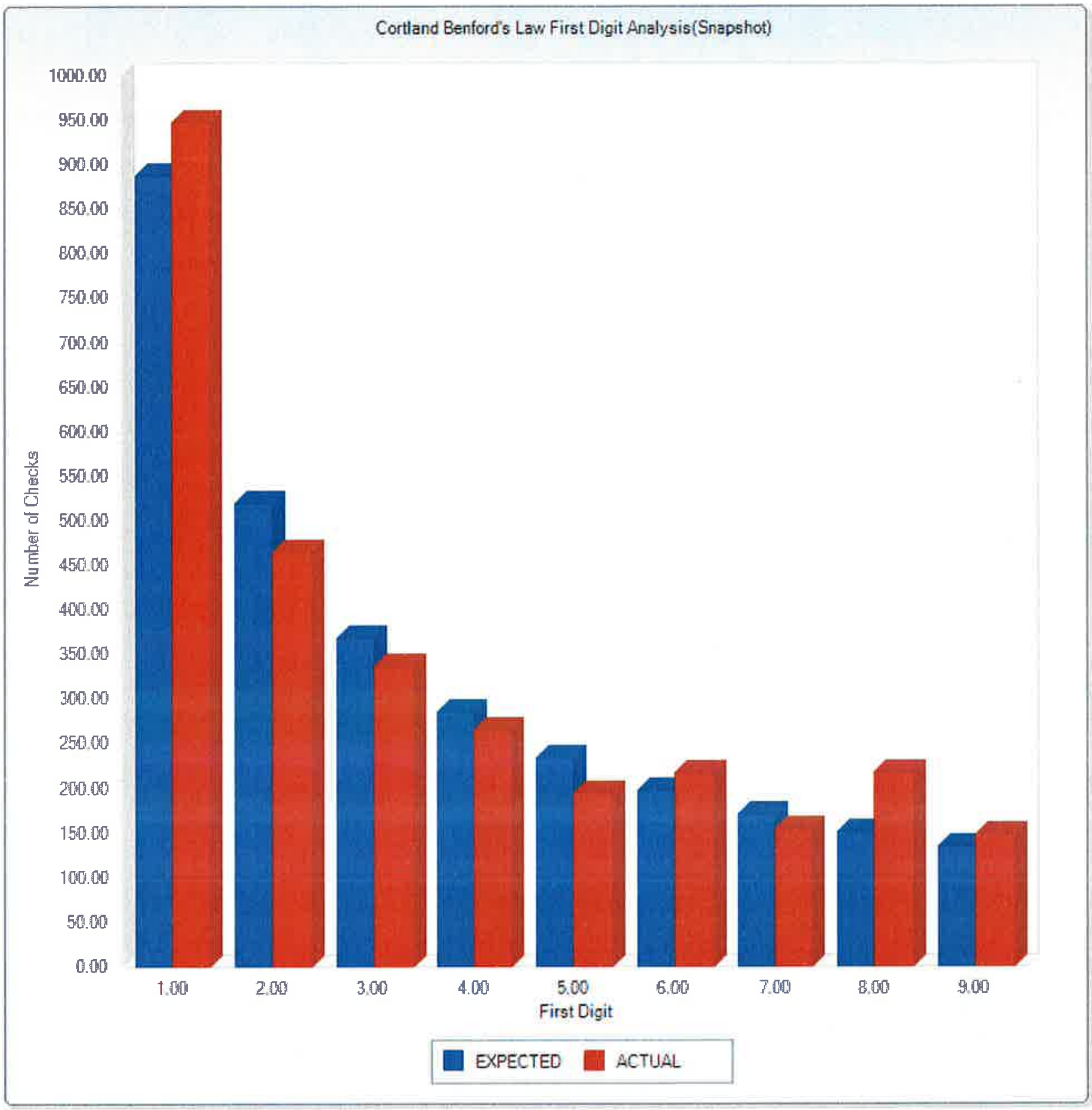
(http://intuitor.com/statistics/Benford's%20Law.html)

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 Districts disbursement journal data for the period of February 1, 2016 through December 1, 2016, the following results were calculated for both the first digit and second digit.

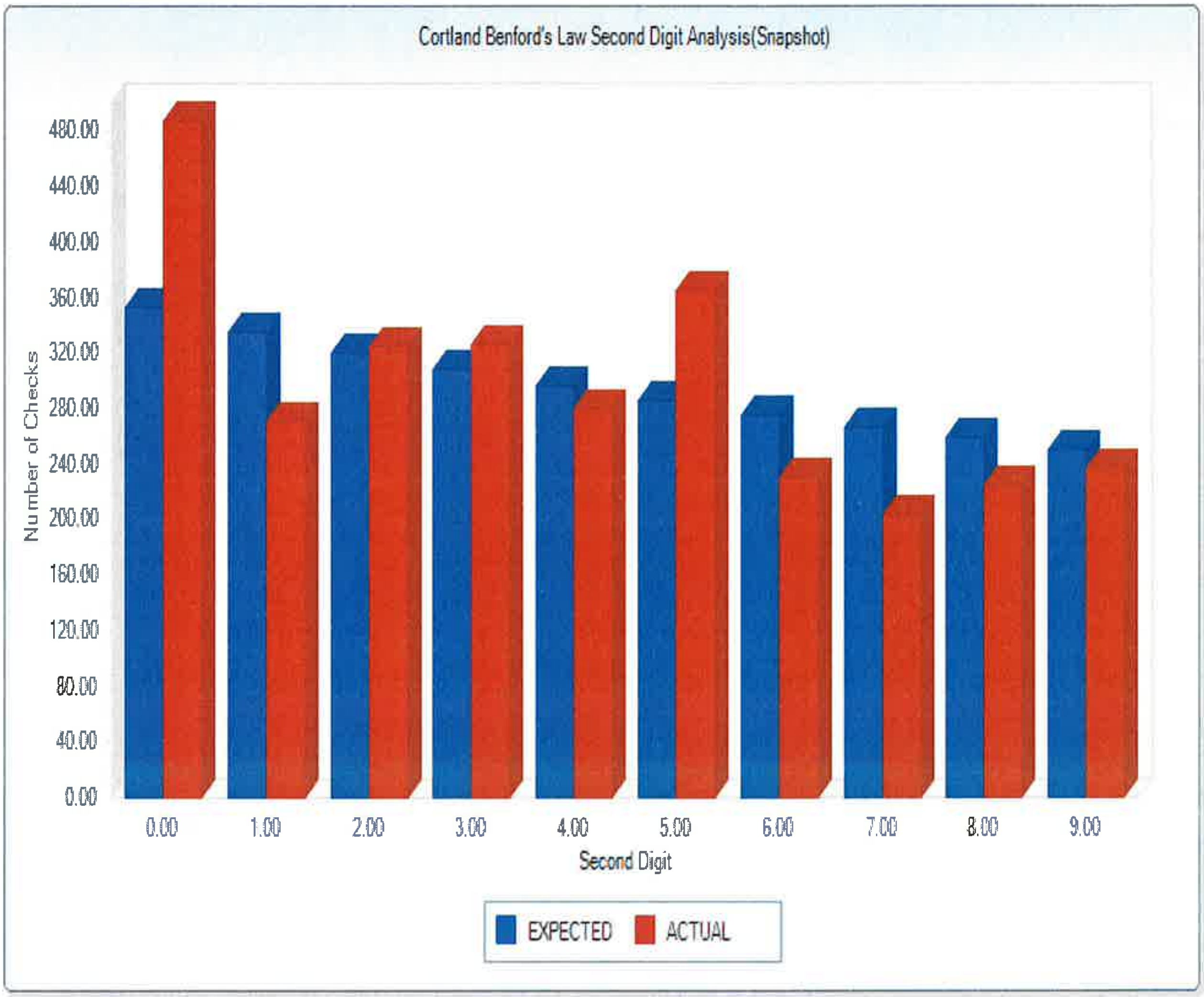
ADDITIONAL TESTWORK PERFORMED



Results for 1st Digit Test

The first digit Benford's Law Analysis showed abnormal variances against the expected counts for the first digits of 1 and 8. The number 1 was associated mainly with employee reimbursements for clothing allowances, dental, and vision insurance. The number 8 was mainly associated with payments for athletic events such as clock operators and referees.

ADDITIONAL TESTWORK 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 and 5". 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 number 5 is mainly associated with athletic event payments as well as athletic dues and association fees.

ADDITIONAL TESTWORK PERFORMED

Duplicate Payment and Gap Detection Test:

Objective

To ensure that all payments made by the district are only made once, and that there is a logical sequence of checks issued. In addition any check gaps can 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 February 1, 2016 through December 1, 2016. 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 were made during the time period tested.

We also utilized this check listed 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.