BALDWINSVILLE CENTRAL
SCHOOL DISTRICT

INITIAL RISK ASSESSMENT
AND
ANNUAL TESTWORK

May 18, 2023

TABLE OF CONTENTS

D'Arcangelo & Co., LLP
CERTIFIED PUBLIC ACCOUNTANTS & CONSULTANTS

5000 BRITTONFIELD PARKWAY, BUILDING B SUITE 103, EAST SYRACUSE, NY 13057

T 315-475-7213 F 315-475-7206

Board of Education and Audit Committee
Baldwinsville Central School District

We have been engaged to assist the Baldwinsville Central School District in performing an the initial risk assessment and annual test work for the year ended June 30, 2023 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 Baldwinsville Central 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 Baldwinsville Central 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

May 18, 2023

East Syracuse, New York

METHODOLOGY

The internal audit process for Baldwinsville Central 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. The District has defined its objectives through its overall mission and vision.

Mission

The Baldwinsville Central School District's mission is to provide leadership, guidance, and resources to help our schools meet the educational needs of all students.

Vision

The Baldwinsville Central School District's vision is to provide educational programs and enrichment opportunities that encourage each child to achieve academic and personal excellence. Our students must attain the intellectual and emotional growth necessary to be successful and independent thinkers, effective communicators, responsible citizens and life-long learners.

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

METHODOLOGY

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.
- *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.

METHODOLOGY

- *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.

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 MAY 18, 2023

		Initial Risk Assessment													
Business Unit	Process	Inherent Risk				Control Risk				Testwork Performed					
		As of May 18, 2023													
		Severe	High	Mod	Low	Severe	High	Mod	Low	2023	2024	2025	2026	2027	Reference
Governance	General Policy and Procedures	✓					✓								
	Monitoring	✓						✓							
	Organizational Structure	✓						✓							
	Risk Management	✓						✓							
Information Technology (IT)	Network Security		✓					✓							
	Financial Application Security		✓					✓							
	Miscellaneous Application Security		✓					✓							
	Disaster Recovery		✓					✓							
	Governance		✓				✓								
Budget	Development	✓						✓							
	Presentation/Compliance	✓						✓							
	Monitoring	✓						✓							
	Amendments			✓				✓							
Financial Reporting	Monthly Reporting	✓						✓							
	General Accounting		✓					✓							
	Annual Reporting		✓					✓							
	Financial Oversight		✓					✓							
	Fund Balance Management		✓					✓							

RISK REGISTER AS OF MAY 18, 2023

		Initial Risk Assessment													
Business Unit	Process	Inherent Risk				Control Risk				Testwork Performed					
		As of May 18, 2023													
		Severe	High	Mod	Low	Severe	High	Mod	Low	2023	2024	2025	2026	2027	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 MAY 18, 2023

Business Unit	Process	Initial Risk Assessment								Testwork Performed					
		Inherent Risk				Control Risk									
		As of May 18, 2023													
		Severe	High	Mod	Low	Severe	High	Mod	Low	2023	2024	2025	2026	2027	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 MAY 18, 2023

Business Unit	Process	Initial Risk Assessment								Testwork Performed					
		Inherent Risk				Control Risk									
		As of May 18, 2023													
		Severe	High	Mod	Low	Severe	High	Mod	Low	2023	2024	2025	2026	2027	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			✓					✓						

CURRENT YEAR'S 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 judgement. For each of the risk areas highlighted, we included a recommendation for the School District to consider in addressing the specific risk.

Governance-General Policy and Procedures

Accounting Procedures Manual

Observation

The District does not have a formalized accounting procedures manual or an inventory of its internal controls and procedures. 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 employees 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.

Recommendation

We recommend that the District develop a comprehensive accounting procedures manual that is separate from Board Policy and Superintendent Regulations. 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.

CURRENT YEAR'S RISKS AND RECOMMENDATIONS

- 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.

Conflict of Interest Statements

Observation

Currently the Board of Education and cabinet members are 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 employees' decision. This process could be strengthened by adding a section for a reviewer to sign off on as reviewed for any potential threats.

Recommendation

We recommend the District add a reviewer signoff to form, and formalize a procedure to document communication of the results to the appropriate individual.

CURRENT YEAR'S RISKS AND RECOMMENDATIONS

Information Technology - Governance

State Privacy Regulation Implementation

Observation

Project initiatives were established at the District with objective of meeting the requirements set forth within the NYS ED Section 2-d Regulation Part 121 (referred to as 2-d) for Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information

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

- Establishing a parents' bill of rights for data privacy and security which includes all the required 2-d components that is posted on the district's website
- Breach reporting and compliant handling procedures
- Designating a Data Protection Officer (DPO)
- Identifying data which is inscope for 2-d
- Conducting analysis of District's security and privacy controls based on NIST CSF
- Tracking of all vendors which are inscope for 2-d

The District has used the BOCES templates to conduct an analysis of their security and privacy controls based on the NIST CSF requirements. The next step is to consolidate the gaps and establish remediation plans. Other project initiatives which are based upon the NIST CSF implementation is comprised of establishing District standards for data protection and privacy which the District has started along with inventorying all District resources based on a data classification standard. It should be noted the District had previously established a matrix to classify specific data at the District which will be further expanded to cover these NIST CSF requirements.

The District is currently following up with the few vendors they have direct contracts with to request contract amendments which meets 2-d requirements. However, the model contract used by the District is missing 2-d required clauses related to data breach handling and requiring vendors to establish data security and privacy policies which they will make available to the School District upon request.
The NYSED schedule ED-1 data retention requirements have been replaced with the LGS 01 standard. These retention requirements relate to specific IT activity, and instructional & District business activity which would be retained on systems that are managed in most cases by third-party vendors. The District has not established a project initiative to interpret these requirements and formally document retention requirements for electronic and paper retention of these interpreted components. The District has performed an analysis of the ED-1 requirements which will be applied to the updated LGS 01 retention standard.

CURRENT YEAR'S RISKS AND RECOMMENDATIONS

Recommendations

1. Proceed with the remaining NIST CSF framework implementation project initiatives consisting of establishing a consolidated control gap list and remediation plans.
2. Continue with initiatives to establish for data protection and privacy standards
3. Proceed with establishing a data classification standard and determine data classifications assigned to applications and IT Services used by the District.
4. For the critical vendors which host District inscope 2-d data, in which the District has a direct contract with these third parties (i.e., excludes contracts that BOCES manages in which they include a required 2-d contract clauses), submit a contract amendments to these vendors which includes the missing 2-d required provisions.
5. Establish a project to interpret the LGS 01 standard from a business and Instructional record standpoint to determine which applications systems would be subject to data retention requirements. For any of the application that are hosted by third-party vendors, the District should send a formal communication to question whether they are meeting the LGS 01 retention requirements. In addition, IT should confirm the retention of data for IT areas directly under their responsibility.

Information Technology - Governance

Vendor Management

Observation

The District is reliant on third parties to operate critical applications in use at their facilities. In order to assess the effectiveness of the controls within these externally hosted operations, it is industry best-practice for these hosting vendors to undergo an independent control evaluation such as the AICPA's Statement on Standards for Attestation Engagements No. 18 (SSAE 18) and Attestation Standards Section 101 (AT Section 101) in order to provide visibility within these service providers' control design (i.e., referred to as a SOC 1 and SOC 2 reviews).

The District utilizes the WinCap 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, and NutriKids to handle the cafeteria services. These applications are hosted by BOCES (CNYRIC) along with providing the District's internet access
. BOCES has complete responsibility for managing the application, network connectivity, system operations and security. BOCES has completed a 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 uses VersaTrans for managing its student transportation operations. VersaTrans is hosted at the vendor's (Tyler Technologies) location. The vendor has formally stated that they

will not undertake a SOC review but conducts self-assessments to validate their compliance with the NIST CSF framework which is recognized as the accepted standard within 2-d

At the start of the Risk Assessment School Tool was operating within the BOCES (CNYRIC) environment and was moved recently to the School Tool (Mindex Technologies) vendor's managed environment. CNYRIC has formally stated that they will continue to address any security matter with Mindex. This will include the assurance of Mindex adherence to 2-d and performing a vendor oversight review using a questionnaire that is aligned with NIST 800-52 r5. In addition, CNYRIC stated that they will request confirmation of their annual risk assessment conducted by the third party and any information that can be shared from that assessment without compromising the security of Mindex.

Recommendations

1. The District should request access to this SOC 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. This review should be formalized using pre-defined criteria.
2. The District should perform vendor oversight review of Tyler Technologies using predefined criteria which would need to be established.
3. Review the results of the CNYRIC vendor oversight review of Mindex Technologies when they are available for review for formal District acceptance.

Information Technology - Governance

Security Awareness

Observation

All District staff are required to complete security awareness training (i.e., includes email phishing information) which includes tracking of participation through a professional training delivery service. The District performed an email phishing test three years ago, but these types of tests should be performed on at least an annual basis. The District has contracted with a firm to perform an email phishing test of the District's staff.

Recommendation

Proceed with plan to conduct additional email phishing tests to ensure the District's staff does not fall prey to phishing attacks.

CURRENT YEAR'S RISKS AND RECOMMENDATIONS

Acceptable Use of Technology Resources

Observation

An acceptable use policy (AUP) was developed that addresses both staff and student use. The staff acknowledge their review of AUP. 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.

Recommendation

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

Information Technology -Miscellaneous Application Security

Application Logon Security

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 security monitoring process.

NutriKids is a Heartland Solutions product used to manage cafeteria services which is hosted at BOCES (CNYRIC). The following logon security issues were identified within the NutriKids application:

- No ability to change passwords on a periodic basis
- Only a minimum of 4 characters required in a password
- No lockout or temporary suspension of account after successive invalid login attempts to prevent the unauthorized takeover of an account

School Tool is that application the District uses to manage Student Information. At the time of the Risk Assessment this system was hosted at BOCES. Logon security to the School Tool environment which uses the District's Active Directory (AD) Group Policy settings for logon security which is hosted On-premises at the District. At the time of the Risk Assessment, testing disclosed that the AD Group Policy of suspending an account for 30 minutes after 10 invalid logon attempts was not functioning. Therefore, an unlimited number of unauthorized attempts could be made to access the School Tool system. Since School Tools is designed to be accessible from the Internet, the need to prevent unauthorized takeover of accounts is an important control. It should be noted that since the completion of the Risk Assessment fieldwork, BOCES has

migrated the District's School Tool system to the vendor's environment in which the vendor (Mindex Technologies) is completely responsible for maintaining the security and application support. The District's contract will continue to be managed by BOCES.

Recommendations

1. The District is exploring the possibility of migrating the cafeteria services to Mosaic which has advanced logon security capabilities. The District will be requesting a report from Heartland Solutions which provides a list of invalid logon attempts which would be reviewed by the District.

2. The District is working on alternate solutions to provide more effective School Tool logon security controls In the interim, to mitigate the risk, the District has established a logging process to capture invalid logon attempts and will use AlienVault SEIM to initiate alerts to IT for their follow up analysis to identify potential brute force attacks in the attempt to takeover District School Tool accounts.

Information Technology - Disaster Recovery

Disaster Recovery Planning

Observation

The Baldwinsville Central School District has developed a comprehensive Disaster Recovery and Business Continuity plan which focuses on components of the Business Impact Analysis which defines Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for applications systems which the District uses. In addition, the District has developed a comprehensive Cybersecurity Incident Response Plan.

The District has migrated all of its financial business, transportation student information and Special Education systems to vendor hosted environments. The systems operating at the District's Data Center located at the Operations Building is comprised of the District's Windows domains which manages the camera systems, managing the HVACs, managing the District's building automated locks and the file share which is used by IT and the business office staff. However, the availability of the District's Windows Domain network is critical since the School Tool Student Information system, which is hosted at the vendor location, needs to connect to the District's network environment for authentication to logon to School Tool system.

The server room does have a backup generator which reduces the likelihood of a site issue based on a power distribution. Although the Avaya phone system master controller is located in the server room, since the outside phone lines terminates in the District Office, which does not have a backup generator in the event of a power failure, the District phone system will be operational internally (i.e., no calls can be made to outside or calls incoming to the District).

CURRENT YEAR'S RISKS AND RECOMMENDATIONS

The District completed a Business Impact Analysis (BIA) within its Disaster Recovery Plan. The BIA includes Recovery Time Objectives (RTO) which is the amount of time which key District systems hosted by third parties need to be recovered. For all applications a recovery time of eight hours is defined. However, the District has not performed a validation of whether the vendor hosted application systems are committed to meetings this RTO.

Recommendations

1. Since the District building network design are point to point from each building to the Data Center, establishing an alternate processing site would not provide the typical benefits because all buildings would need to have network capabilities built out to reach this alternate site. Therefore, an analysis should be performed of how an alternative Active Directory environment can be established to allow for School Tool logon authentications to occur when the District's Data Center is not accessible
2. Consider deploying a backup generator at the District Office to ensure the phone system remains operational in the event of a power failure. Alternatively, the connections can be moved from the District Office to the server room.
3. Contact vendors which host District systems and obtain formal RTO commitments to determine whether they meet stated District RTO requirements. For any instances in which these vendors are not able to meet the District's RTO requirements, this risk should be escalated to the Audit Committee for possible risk acceptance.

Information Technology- Network Security

Physical Security to Data Center

Observation

The District's Data Center is located in the building used by the Special Education Department. There is an external door leading to the data center which is controlled by card key access. However, there is another door that opens to the Special Education office space. This door is an emergency exit door and must remain available. There are IP cameras within the Data Center which would monitor all activity and cameras are pointing to the outside door. In addition, all systems require logon security access to use these systems.

The Data Center is located in parking lot where past water leakage issues have been repaired. The equipment is located in equipment racks that are not raised which makes the equipment suspectable to water damage.

CURRENT YEAR'S RISKS AND RECOMMENDATIONS

Recommendations

1. The District should install water sensors in the data center which provides alerts when there is water on the floors.

2. The District should invest in racks where all equipment can be raised.

3. The District should consider installing alarms when the door leading to the Special Education offices is opened.

Network Vulnerability Management

Observation

The District's has installed an industry leading solution, Crowdstrike for managing its servers and endpoints. In addition, the District has implemented a SIEM to collect server logs and provide alerts of suspicious security activity. The District has an effective security patch deployment program using a Microsoft Solutions which is deployed from a District managed Azure environment.

The only remaining area of security consideration is to perform annual vulnerability assessments of the District's external facing environment. The last vulnerability assessments were performed in 2019. The external facing environment is solely to provide the District internet access, allow VPN access to a limited number of support staff personnel and to support the School Tool vendor hosted connection requirements to perform the School Tool Logon authentication.

Recommendation

Run an industry accepted vulnerability scanner to identify any security vulnerabilities identified within the District's external IPs and apply any required remediation.

RESULTS OF ANNUAL TEST WORK

EXECUTIVE SUMMARY

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, receiving 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, 2022 through January 31, 2023. We randomly selected One Hundred-Fifty (150) disbursements for testing.

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

- 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 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.
- Verify disbursement was signed off by the internal claim's auditor.

Results:

Based on our procedures performed the internal controls in the accounts payable/purchasing department are properly designed and are being followed. No corrective action is needed.

Although internal controls are properly designed, we recommend the following best practice s to further strengthen internal controls.

EXECUTIVE SUMMARY

Purchasing/AP-Procurement Process

Receiving of Goods

Observation:

During our inquiry/review of the procurement process we noted that goods are received by the individual buildings and distributed to the individual that requisitioned the goods. The receiving documentation needed by the accounts payable clerk is delayed by the fact that the documentation is not remitted to the accounts payable department even though the goods have been received. This results in additional time tracking down the documentation by the account payable clerk.

Recommendation:

We recommend the District consider a centralized receiving process, or that each building designate a person responsible for the receiving of goods into the building. Once received into the building the receiving documentation should be signed and remitted to the accounts payable clerk. The goods can then be distributed to the individual that requisitioned the goods.

EXECUTIVE SUMMARY

Vendor Change Reports

Observation:

During our inquiry/review of the procurement process we noted that vendor change reports are not being generated and reviewed by a designated individual outside of the accounts payable process.

Recommendation:

We recommend that the District designate an individual to review vendor change reports on at least a monthly basis. This would add a level of monitoring control and further mitigate the risk on the accounts payable process.

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 seven (7) 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, 2022 through January 13, 2023. 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 results 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 seven (7) 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 recommendations based on results 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

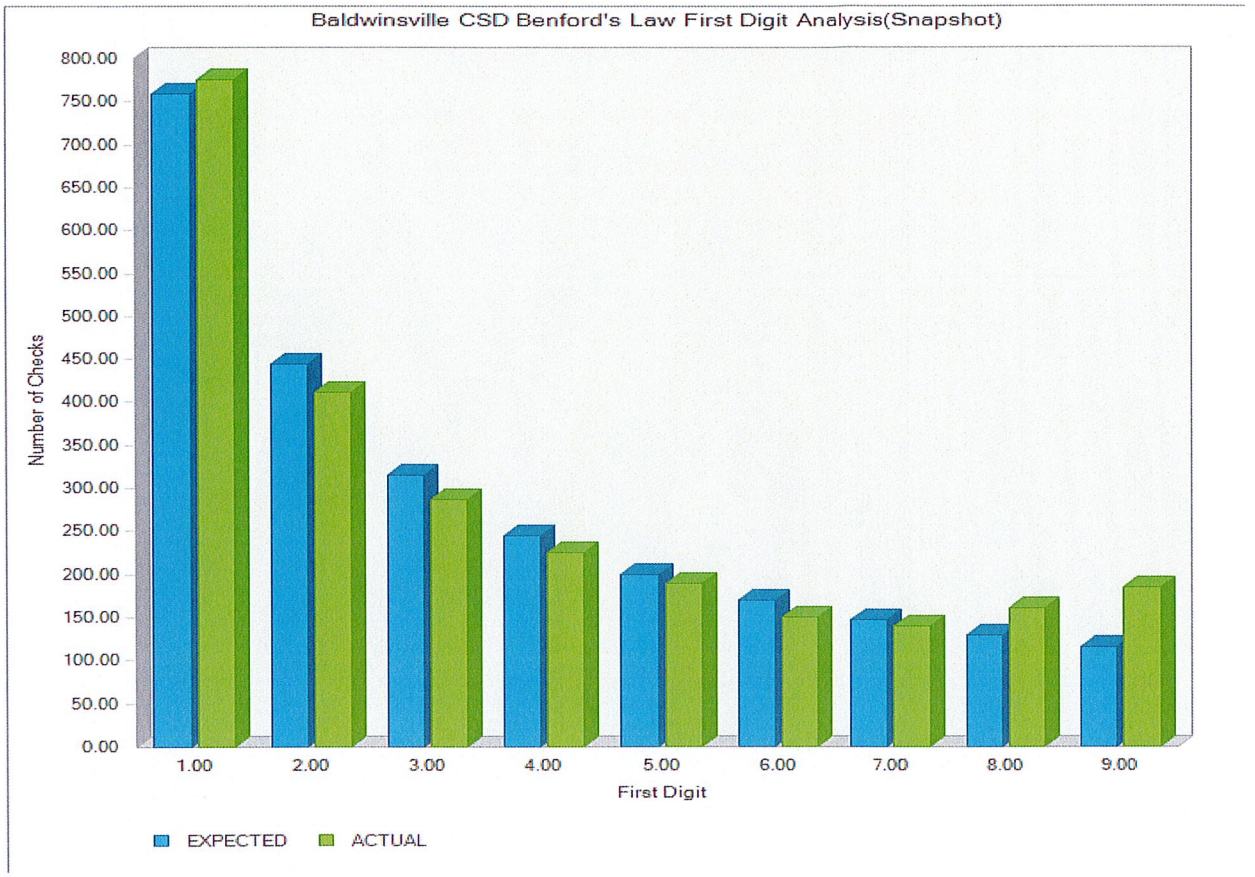
(http://intuitor.com/statistics/Benford's%20Law.html)

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 July 1, 2022 through January 13, 2023; the following results were calculated for both the first digit and second digit.

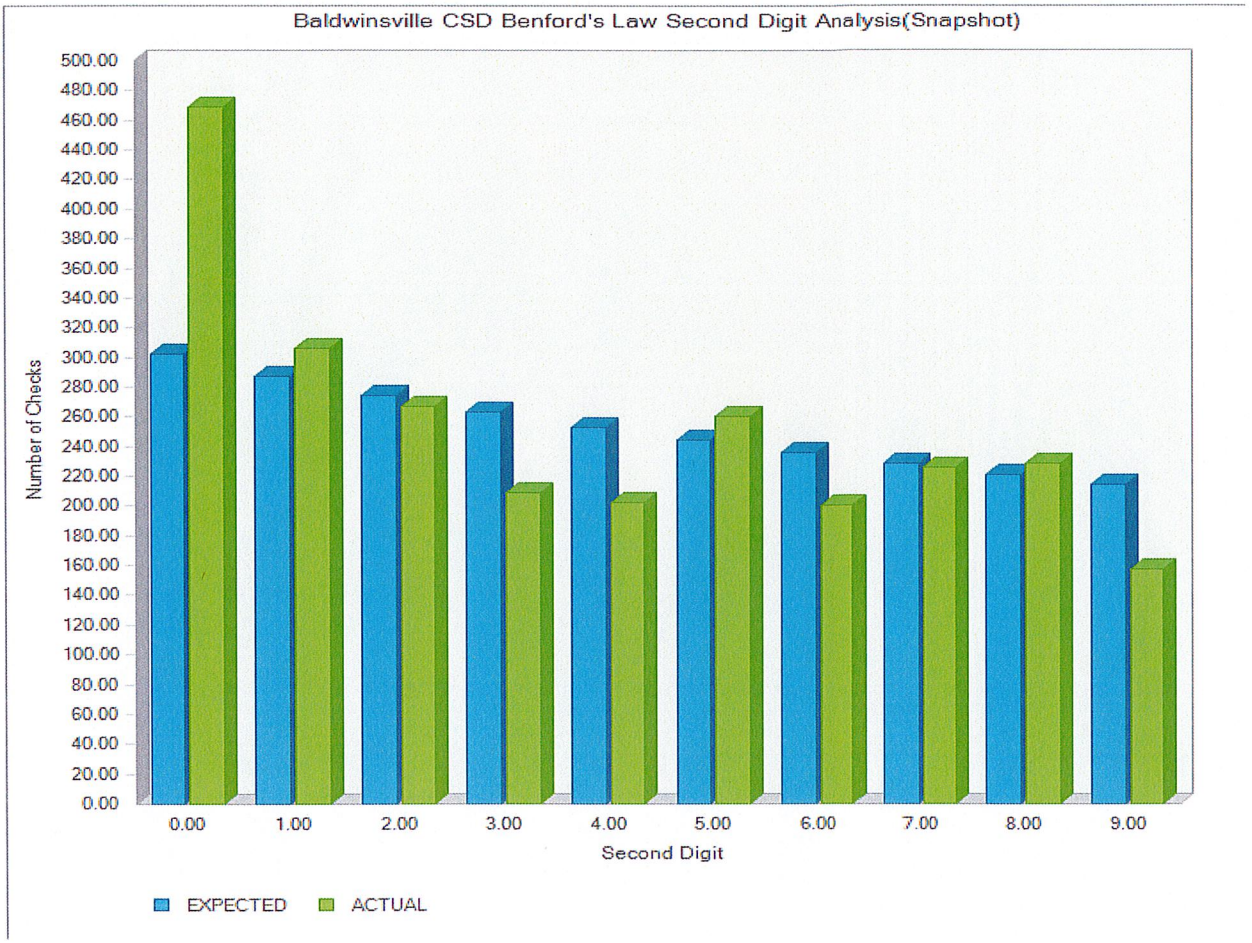
ADDITIONAL TESTWORK PERFORMED



Results for 1st Digit Test

In performing the first digit Benford's law Analysis we saw a higher than expected number of check amounts starting with "1, 8, and 9." The first digit "1" can be explained largely by payments to sports officials, supply purchases, and by individual recurring payroll deductions. The digits 8, and 9 can be explained by payments to sports officials as well as refunding of AP exam fees.

ADDITIONAL TESTWORK PERFORMED



Results for 2nd Digit Test

In performing the second digit Benford's law Analysis we saw a higher than expected number of check amounts with the second digit of "0, 1, 5, and 8". The second digit 0 can be explained by a large number of even dollar checks for contractual payments. For example, 100, 200, 500, 1,000.