CORTLAND ENLARGED
CITY SCHOOL DISTRICT

INTERNAL AUDIT

RISK ASSESSMENT UPDATE
AND
ANNUAL TESTWORK

December 15, 2023

Cortland Enlarged City School District

TABLE OF CONTENTS

Board of Education and Audit Committee
  Cortland Enlarged City School District

We have been engaged to assist Cortland Enlarged City School District in performing an update to the initial risk assessment and annual test work for the year ended June 30, 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 the standards required by the Regulations of the Commissioner of Education.

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

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

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

D'Arcangelo + Co., LLP

December 15, 2023

Rome, New York

METHODOLOGY

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

Defining Audit Universe

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

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

Weighting of Business Units

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

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

METHODOLOGY

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

Defining Business Unit Processes

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

Categories of Risk

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

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

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

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

METHODOLOGY

Assessing a Risk Level

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

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

Risk Appetite

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

Managing the Risk

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

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

Audit Plan

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

RISK REGISTER AS OF December 15, 2023

Business Unit	Process	Inherent Risk				Control Risk				Testwork Performed						Reference
		Risk Assessment Update — As of December 15, 2023														
		Severe	High	Mod	Low	Severe	High	Mod	Low	2018	2019	2020	2021	2022	2023	Reference
Governance	General Policy and Procedures	✓					✓									
	Monitoring	✓						✓								
	Organizational Structure	✓						✓								
	Risk Management	✓						✓								
Information Technology (IT)	Governance/Security		✓				✓						✓			
	Financial Application Security		✓					✓					✓			
	Network Security		✓					✓					✓			
	Miscellaneous Application Security		✓					✓					✓			
	Disaster Recovery		✓					✓					✓			
Budget	Development	✓						✓								
	Presentation/Compliance	✓						✓								
	Monitoring	✓						✓								
	Amendments			✓				✓								
Financial Reporting	Monthly Reporting	✓						✓								
	General Accounting		✓					✓								
	Annual Reporting		✓					✓								
	Financial Oversight		✓					✓								
	Fund Balance Management		✓					✓								

RISK REGISTER AS OF December 15, 2023

Business Unit	Process	Inherent Risk				Control Risk				Testwork Performed						
		As of December 15, 2023														
		Severe	High	Mod	Low	Severe	High	Mod	Low	2018	2019	2020	2021	2022	2023	Reference
Payroll/HR	Payments to Employees	✓						✓				✓				
	Allocation of Expenditures	✓						✓								
	General Employee Administration		✓					✓				✓			✓	Page 18
	Employee Benefit Administration	✓						✓							✓	Page 18
	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 December 15, 2023

Business Unit	Process	Inherent Risk				Control Risk				Testwork Performed						Reference
		As of December 15, 2023														
		Severe	High	Mod	Low	Severe	High	Mod	Low	2018	2019	2020	2021	2022	2023	
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 December 15, 2023

Business Unit	Process	Inherent Risk (As of December 15, 2023)				Control Risk				Testwork Performed						Reference
		Severe	High	Mod	Low	Severe	High	Mod	Low	2018	2019	2020	2021	2022	2023	
Transportation	Fleet Maintenance			✓				✓								
	Risk Management		✓					✓								
	Personnel Compliance			✓				✓								
	Facilities Maintenance and Security		✓					✓								
Cash Receipts/ Billing	Real Property Tax	✓						✓								
	Medicaid		✓					✓			✓					
	Out of District Tuition			✓				✓								
	Use of Facilities			✓				✓								
	Admissions and Concessions		✓					✓								
	Donations			✓				✓								
	Collection/Posting of Receipts		✓					✓								
Extraclassroom	General		✓					✓		✓						
	Cash and Cash Receipts		✓					✓		✓						
	Expenditures and Purchasing			✓				✓		✓						
	Inventories			✓				✓		✓						

PRIOR YEAR RISKS AND RECOMMENDATIONS

2015-01 *Accounting Procedures Manual*

Prior Year Observation

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

Prior Year Risk

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

Prior Year Recommendation

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

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

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

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

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

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

PRIOR YEAR RISKS AND RECOMMENDATIONS

Current Year Status:

The District is in agreement with this recommendation and has started to compile business office procedures into a google shared folder. No corrective action necessary.

2017-02   *Uniform Guidance Procurement Policies*

Prior Year Observation

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

Prior Year Risk

The District will not be in compliance with Federal Grant regulations

Prior Year Recommendation

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

Current Year Status:

The District has updated its procurement policy in accordance with Uniform Guidance. The documentation of procurement procedures over compliance in accordance with Uniform Guidance is in process.

Current Year Recommendation

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

PRIOR YEAR RISKS AND RECOMMENDATIONS

Information Technology - Governance

2020-04 State Privacy Regulation Implementation

Prior Year Status

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

Based on the review of ED-2 contract that the District sends to its vendors it did not include the required clauses relating required to data breach notifications to the District.

The District has utilized the BOCES services to provide a template and a strategy to implement the NIST CSF framework. The District has been participating in BOCES organized workshops to assist in determining the District's compliance. These workshops and final District determination of NIST compliance is expected to be completed during the next year which will include establishing a list of gaps and remediation strategies.

Prior Year Recommendation

1. Procced with the remaining validation of the BOCES portal to ensure that it addresses all the vendors they contract through BOCES.

2. The District should submit these potential missing ED-2 clause to their lawyer to determine whether additional revisions are needed.

3. Proceed with project initiatives to assess the District compliance with the NIST CSF framework and establish remediation projects for any identified gaps.

Current Year Status

1) **The District performed the validation to ensure all their vendors they have managed BOCES are reflected in their tracking for ED-2 contract updates**

2) **ED-2 clause has been identified and incorporated into the updated contracts. There are 20 instructional software in use where the District has direct contract with vendors are in scope for ED-2 data. All other contracts are through BOCES who maintains the responsibility for having ED 2 compliant contracts in place with these software vendors. We verified a sample number of these contract to verify that the ED-2 clause was included in the newly executed agreements.**

PRIOR YEAR RISKS AND RECOMMENDATIONS

3) **NIST CSF framework developed by BOCES is in the evaluation phase to determine maturity levels for each of the control. Upon completion, it will be necessary to identify gaps and develop a remediation plan which will include data protection and privacy related standards as required by ED-2.**

Current Year Recommendation

Proceed with plans to complete NIST CSF gap analysis, develop remediation plans, and establish data protection and privacy related standards as required by ED-2.

2018-01   *Vendor Management*

Prior Year Status

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

The District utilizes the nVision IS application to handle financial processing (i.e., payroll, vendor check disbursements and maintaining the general ledger) and IEP Direct to handle its Special Education program, and NutriKids to handle the cafeteria services. These applications are hosted by BOCES (CNYRIC) along with providing the District's internet access and website. BOCES has complete responsibility for managing the application, network connectivity, system operations and security.

BOCES recently completed a SSAE 18 service SOC 2 Type 2 audit in which BOCES established a restricted process in order for School Districts to have the opportunity to review this report.

Prior Year's Recommendation

The District should request access to this report from CNYRIC to ensure the services they use were included in the scope of the audit and all existing exceptions identified in the report presented no risk to the District.

Current Year Status

The District has approached CNYRIC to provide them access to the SOC 2 report which requires the District to go onsite to perform this review.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Current Year Recommendation

Proceed with plans to obtain access to the SOC 2 report and complete a formal review using pre-defined criteria.

2015-04 *Data Classification*

Prior Year Status

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.

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

Prior Year Recommendation

Proceed with plans to implement a data classification framework.

Current Year Status

This will be implemented as one of the final tasks as part of the NIST CSF implementation.

Current Year Recommendation

Develop and implement a data classification framework as part of the NIST CSF implementation.

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

Prior Year Status

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.

The records management officer retired this past year. As of July, 2021 a new records management officer and records access officer has been appointed. This initiative will be

PRIOR YEAR RISKS AND RECOMMENDATIONS

addressed during this upcoming year which will include establishing the District's interpretation of ED-1 data retention requirements and implementing the required storage solutions.

Prior Year Recommendation

Proceed with plans to implement data retention requirements which meets ED-1 requirements.

Current Year Status

The ED-1 data retention requirements have been replaced with the LGS 01 standard. These retention requirements relate to specific IT activity, instructional and business activity which would be retained on systems that are managed in most cases by external vendors

An interpretation of these requirements are required from an instructional, business office and IT perspective is next project initiative.

Current Year Recommendation

Proceed with plans to interpret these requirements as required from an instructional, business office and IT. The next step would be to identify location of data to determine whether retention requirements are being met.

2019-01   *Security Awareness*

Prior Year Status

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

Prior Year Recommendation

Proceed with the evaluation to implement an email phishing test program.

Current Year Status

The IT Director is evaluating several alternatives to perform phishing simulation test exercises.

Current Year Recommendation

Proceed with plans to complete evaluation at which time budget decisions will be made.

PRIOR YEAR RISKS AND RECOMMENDATIONS

Information Technology – Miscellaneous Application Security

2020-03 Application Logon Security - Transfinder

Prior Year Status

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

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

Prior Year Recommendation

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

Current Year Status

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

Current Year Recommendation

District should consider establishing formal criteria to conduct a vendor oversight review.

Information Technology - Disaster Recovery

2015-06   *Contingency Plan*

Prior Year Status

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

PRIOR YEAR RISKS AND RECOMMENDATIONS

Prior Year Recommendation

Establish a project initiative to create a Business Impact Analysis for all critical District applications.

Current Year Status

The District has not proceeded with this project initiative.

Current Year Recommendation

Create a Business Impact Analysis for all critical District applications.

Information Technology – Financial Application Security

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

Prior Year Status

The District's processes include the assignment of user security entitlements to application systems based on an individual's job requirements. The access is generally assigned either through predefined security roles or customizing the access of users with unique access requirements based on their individual job function. It is industry best practice to perform an annual recertification that individuals are assigned the proper access based on the requirements of their job function. Past efforts to perform an effective recertification process were limited due to the lack of reports that are provided by nVision.

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

Prior Year Recommendation

Proceed with plans to evaluate the security design of nVision roles to support an effective recertification process.

Current Year Status

The current access recertification performed by the business administrator is comprised verifying only active employees have access to nVision. The business administrator has knowledge of the resource roles and what job functions function requires access to these

PRIOR YEAR RISKS AND RECOMMENDATIONS

roles. The business administrator has expanded the access recertification process during this school year to select a subset of the total users each year to validate whether their assignment to resource roles is appropriate based on the requirements of their job function.

Current Year Recommendation

None

2022-02 Acceptable Use of Technology Resources

Prior Year Status

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

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

Prior Year Recommendation

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

Current Year Status

The policies were last updated in 2019 and while some provisions exist for social media use, it is not a broad based set of policies relating to cloud based technology use. The audit team has provided a set of guidelines to address these areas more specifically.

Current Year Recommendation

Update the AUP to more broadly govern the use of cloud based technologies.

RESULTS OF ANNUAL TESTWORK

EXECUTIVE SUMMARY

D'Arcangelo & Co., LLP was requested by the *Cortland Enlarged City School District* Board of Education and the Audit Committee to conduct procedures over internal controls related to employee benefit deductions for employees. The following summarizes the results of the procedures performed in those areas.

Employee Benefit Administration

Objective and Procedures Performed

The objective of the engagement is to evaluate the District's internal controls related to employee benefit administration

Our procedures were as follows:

- Reviewed the District's policies, procedures, and practices with regards to internal controls over the processing of employee benefits for employees and retirees.
- Interviewed key District employees involved in the employee benefits process
- Tested a sample of sixty-five (65) employees who received benefits during the period July 1, 2022 through June 30, 2023 to ensure benefit was in agreement with the employment contract and the employees' payroll deductions were properly calculated.

Outcome of Procedures Performed

Based on the results of our test work the following are recommendations based on the outcome of our procedures"

Calculation of Employee Deductions

Based on the recalculation of employee deductions for the sixty five (65) employees sampled, six (6) were found six (6) to have discrepancies totaling $324.74. This discrepancy had been discovered by District personnel and was corrected in July 2023. The discrepancy was related to the CSEA bargaining unit and resulted in approximately $6,753 in overpayments.

Recommendation

We recommend the District develop an oversight process at the beginning of the year to review deduction amounts for all employees to ensure amounts are correct.