



Williamsville Central School District
Risk Assessment and Internal Audit Plan

January 30, 2025

January 30, 2025

Audit Committee
Assistant Superintendent of Finance
Williamsville Central School District
105 Casey Road
Williamsville, New York 14051

Dear Audit Committee:

This report, as expressed in the risk assessment ratings, provides you, the District's management, and the audit committee with the assessment of the need for controls and a means to prioritize risk mitigation efforts. The risk assessment is an initial step in your risk management program of assessing risk, evaluating controls, reviewing control effectiveness, and adapting measures to achieve an acceptable level of risk. The risks noted in the risk assessment should be evaluated in light of your existing policies and practices to identify potential improvements or changes in the control structure based on the level of risk presented. To assist you in establishing review programs for these activities, a potential audit plan and schedule for the internal audits are provided.

We appreciate the opportunity to prepare this risk assessment for Williamsville Central School District and are available to assist you in carrying out other portions of the risk management program including the work plan. We are also available to answer your questions. Please contact Kathryn Barrett at 585-344-1967 or Katelyn Crowley at 716-362-6281.

Sincerely,



Freed Maxick P.C.

Table of Contents

EXECUTIVE SUMMARY	1
RESULTS OF REVIEW OF INTERNAL CONTROLS AND CONFERENCE CALLS	3
CORRECTIVE ACTIONS TAKEN ON PREVIOUSLY REPORTED FINDINGS	6
RISK ASSESSMENT SUMMARY	7
INTERNAL AUDIT PRIORITIES	9
BUSINESS RISK ASSESSMENT SIGNIFICANT CHANGES.....	10
INTERNAL AUDIT PLAN	11
APPENDIX - RISK CATEGORY DEFINITIONS.....	12

EXECUTIVE SUMMARY

The internal audit function's primary responsibility is to assist the Board of Education in ensuring that control risks are identified and that appropriate internal controls are in place to address those risks. An entity's internal control is a process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance that assets and District information is adequately safeguarded and reduce the likelihood that errors and/or irregularities could occur and go undetected.

In 2006, the audit committee requested that Freed Maxick P.C. perform an initial risk assessment and prepare an internal audit plan for Williamsville Central School District (the District). This report represents an update to the initial risk assessment that was performed for the Williamsville Central School District. It has been updated for all modifications made to the internal controls since the initial risk assessment was performed. This risk assessment and internal audit plan will be used to develop the scope and direction of the internal audit program to be deployed by the District and Freed Maxick P.C. during the current fiscal year.

Establishment of a comprehensive internal audit program will enable the District to align its mission and vision with its operational structure and environment, assess risk as it relates to materiality, opportunity, and organizational objectives, control risk mitigation, improve organizational functionality through value-added communication and information resourcing, and vigilantly monitor the effectiveness of internal control to promptly counteract any shortfalls. It can also be used to determine what resources will be needed to complete the identified higher risk internal audits.

Intrinsic in the risk assessment of the Williamsville Central School District is the concept of materiality. Those areas of the District that deal with more significant dollars or a higher volume of transactions will most likely score as higher risk merely due to the dollars and number of transactions passing through those transaction cycles.

The objective of this report is to ensure that Williamsville Central School District has sufficient and continuous internal audit coverage of those areas judged as having a relatively higher risk profile or that otherwise require internal audit attention for regulatory or management reasons.

The scope of the risk assessment and internal audit plan has been reviewed and approved by the Audit Committee of Williamsville Central School District, who in turn has final responsibility and authority for the satisfactory execution of the internal audit plan. The risk assessment and internal audit plan is primarily risk-based and is organized around the District's major internal control cycles. The plan was developed based on detailed interviews with employees, administrative personnel, the results of previous internal and external audits, and our cumulative knowledge of the District's internal control risks.

Our interviews with employees, management and administrative personnel were directed toward gaining a thorough understanding of the objectives and related risks in each internal control area, from the perspective of the individuals responsible for controlling such risks. Using this information and input, we evaluated the level of risk (low, moderate or high) present in each area; across a standard spectrum of risk categories (see Appendix for risk category definitions). A summary of this risk analysis by control cycle is included subsequently. The risk assessment process also drives the planned scope of the internal audit coverage, which is summarized by internal control area.

District administration and the Audit Committee are responsible for establishing and maintaining effective internal control. Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

RESULTS OF REVIEW OF INTERNAL CONTROLS AND CONFERENCE CALLS

Information Technology:

- ◆ As noted in the prior risk assessment, although employees responsible for IT functions understand their role, responsibilities, and the processes that are to be followed to ensure the District's IT functions operate properly, during our risk assessment we noted many process areas were not well documented and did not clearly communicate to employees responsible for IT functions management's expectations. Formally documented standards for various IT processes helps to ensure employees are aware of their responsibilities related to IT processes and management's intentions regarding implementing those responsibilities. Formal documentation for each IT process should exist. The following are areas where formal documentation could be improved:
 - System Development Life Cycle (SDLC) Policy
 - Information Security Policy
 - Physical Security Management Policy
 - Bring Your Own Device (BYOD) Policy

We recommended the District continue to formally document all IT processes to the extent necessary to ensure employees responsible for IT functions understand their roles and responsibilities, have a consistent process to follow and that the process has been established is consistent with management's expectations. Once these policies and procedures are documented, they should be reviewed at least annually for any updates that are required.

Management Response: The IT Department (reporting to WCSD Leadership) will review and recommend any revisions to these policies prior to the start of the school year.

- ◆ As noted in the prior risk assessment, the District has established certain practices to ensure that users are established with appropriate access rights and access rights are terminated timely as individuals leave the District. Although user access is reviewed annually for the District's accounting system, WinCap, there are other applications that are not reviewed at least annually. This may lead to unauthorized individuals being able to access the systems without being detected. Periodic access reviews are critical to identify if the access provided is commensurate with the user's job responsibilities. An access review can be used to detect scenarios such as: (1) a user with access to certain applications or modules that are not necessary for performance for their daily job responsibilities; (2) access not removed timely for a user that has been separated/terminated from the organization; or (3) a user that has conflicting access rights that can potentially commit fraud (segregation of duties). We recommend access rights be reviewed at least annually for all applications/modules that may be at risk of unauthorized access or that contain personal identifiable information (students and staff) to ensure access to individual applications/modules is appropriate.

Management Response: We understand the importance of reviewing users' access rights. The District has developed the following to aid in this task:

- *Application Dashboard: An inventory of users' access to various programs. This dashboard allows us to easily remove/add program access when a user is no longer employed or transferred to a new position.*

- Accompanying this Dashboard, we have documented the audit procedures to verify various application access. User access to these applications is reviewed twice a year.
- Our Student Management Systems are reviewed periodically throughout the year. Isolating various permissions or roles, we can review access to Student PII.

The District will continue to improve upon these processes and make any necessary adjustments.

- ◆ The data center / server room is located at the District office and Williamsville South High School. Access to the data center / server room is limited to the core information technology staff, however an annual review of server room access is not being performed. The District may be at risk of unauthorized individuals being able to access the data center / server room. We recommend an access review is performed by the District of data center / server room at least annually.

Management Response: Access to the Data Center is achieved through electronic entry. The IT Department will work with Facilities to extract a monthly log of Data Center access to be reviewed by the Director of Technology.

- ◆ As noted in the prior assessment, the District currently has Active Directory lockout parameters configured for 60 invalid attempts. Inadequate lockout parameters could allow a hacker to use brute force and repeatedly attempt to login. Lockout parameters provide enhanced protection against the ongoing threat of a cyber-attack. Freed Maxick recommends the lockout parameters be set to 10 invalid attempts to conform to NIST standards and provide greater protection against unauthorized access. Additionally, the District does not have a control in place to require users to re-authenticate if their session has been idle for more than 15 minutes. We recommend implementing a control to ensure unauthorized users are unable to gain access to any individual's workstation.

Management Response: The District will continue to comply with NIST standards regarding lockout parameters that are applicable to our Active Directory.

- ◆ We noted the IT Department relies on the Human Resources Department to notify them of departures from the District, as well as user access changes. A recent internal audit noted that notification may not occur in a timely manner. If changes are not being made in a timely basis, individuals may have inappropriate access to the District's active directory and system applications. We recommend the District consider establishing an automated notification system to ensure that all changes are communicated and addressed in a timely manner.

Management Response: The District is in development of an automated approach between our Human Resources System and WITS (Williamsville Information Tracking System).

- ◆ While the District provides annual training to its staff regarding cybersecurity awareness that is required by Education Law 2-D, the training does not include a pass/ fail certification that the staff understand the materials presented. We recommend the District implement a questionnaire for the cybersecurity awareness training that requires staff to pass to confirm understanding.

Management Response: The District will continue to provide faculty and staff annual cybersecurity awareness training by following the NYS Ed Law 2D requirements.

- ◆ The District currently does not have a full Business Continuity Plan (BCP) in place but does have a Disaster Recovery plan. The BCP is a plan used by the District to ensure that the business operations continue during an event, emergency, or even a disaster. The development of the BCP usually involves a Business Impact Analysis (BIA) to measure the use, utility, or need of each system to remain running during an event, emergency, or disaster. The BCP is then developed to include items such as: (1) a listing of systems and their criticality; (2) definitions or examples of “events”, “emergencies”, or “disasters”; and (3) detailed plans to continue business or restore business should any of these types of events occur. The District may develop this plan with BOCES, as BOCES generally provide some level of business continuity for the District during an event, emergency, or disaster. We recommend that the District work toward creating a Business Continuity Plan.

Management Response: The District will work in conjunction with BOCES on the development of the Business Continuity Plan.

CORRECTIVE ACTIONS TAKEN ON PREVIOUSLY REPORTED FINDINGS

Information Technology – We noted during our previous risk assessment that the District has not implemented required annual training of employees regarding data privacy and security awareness as part of the Ed Law 2-d compliance. The District has implemented training using GCN as well as a service provider to train on cybersecurity. The training includes questions at the end of the training.

Information Technology – We noted during our previous risk assessment that the Assistant Superintendent for Finance had edit rights for most if not all WinCap modules. The District adjusted the Assistant Superintendent for Finance's WinCap rights to read only for all modules except the budget module and the administrative user access lockout and password reset modules.

RISK ASSESSMENT SUMMARY

Risk Factors>>> (Definitions of the Risk Categories can be found in the Appendix)	Inherent Risk Factors								Control Risk Factors					Current Year Risk Score	Current Year Rating	Prior Year Risk Score
	Ext Mkt Rep	Financial	Operational	Legal/Regulatory	Strategic	Tech/System	People/Culture	Fraud	Monitoring	Info/Communications	Control Activities	Risk Assessment	Control Enviro.			
Budgeting, Governance and Reporting	L	H	L	L	M	L	M	L	S	S	S	S	S	245	2	232
State Aid	L	M	L	L	L	L	L	L	S	S	S	S	S	212	6	212
STAC Processing	L	L	L	L	L	L	L	L	S	S	S	S	S	200	8	200
Medicaid Billing	L	L	L	L	L	L	L	L	S	S	S	S	S	200	9	200
Grants	L	L	L	L	L	L	L	L	S	S	S	S	S	200	10	200
Centralized Cash Receipts	L	L	L	L	L	L	L	L	S	S	S	S	S	200	11	200
Community Education Cash Receipts	L	L	L	L	L	L	L	L	S	S	S	S	S	200	12	200
School Lunch Cash Receipts	L	L	L	L	L	L	L	L	S	S	S	S	S	200	13	200
Purchasing and Cash Disbursements	L	H	L	L	L	L	L	L	S	S	S	S	S	224	3	224
Purchase Cards	L	L	L	L	L	L	L	L	S	S	S	S	S	200	14	200
Payroll Processing	L	H	L	L	L	L	L	L	S	S	S	S	S	224	4	224
Employee Benefits and Paid Time Off	L	M	L	L	L	L	L	L	S	S	S	S	S	212	7	212
General Ledger Maintenance	L	L	L	L	L	L	L	L	S	S	S	S	S	200	15	200
ACH and Wire Transfers	L	L	L	L	L	L	M	L	S	S	S	S	S	213	5	200
Fixed Assets	L	L	L	L	L	L	L	L	S	S	S	S	S	200	16	200
Fuel Depot	L	L	L	L	L	L	L	L	S	S	S	S	S	200	17	200

RISK ASSESSMENT SUMMARY (CONTINUED)

	Inherent Risk Factors									Control Risk Factors									
Risk Factors>>> (Definitions of the Risk Categories can be found in the Appendix)	Continuance of Business	Communications/ Network	Business Units Served	Complexity of Env.	Staffing	Availability/Response	Computing Platform	Information Sensitivity		Monitoring	Info/Communications	Control Activities	Risk Assessment	Control Enviro.		Current Year Risk Score	Current Year Rating		Prior Year Risk Score
Information Technology	L	L	L	L	L	L	L	L		S	S	M	M	M		259	1		258

RISK ASSESSMENT SUMMARY

INTERNAL AUDIT PRIORITIES

Based on this risk assessment the following areas have been identified as high-risk relative to the current fiscal environment and internal controls that existed at the time of our risk assessment. We recommend the Audit Committee consider selecting for internal audit at least one of the areas identified below:

- ◆ Budget, Governance and Reporting - Because of the financial risks budget and reporting practices could have on a district and the Assistant Superintendent of Finance is new to the District and position as of May 2024, this has been identified as an area of higher risk. We will review the budget process and historical budget to actual data to gain comfort that the budgets developed by the District are reasonable. We may review the District's calculation of the property tax cap. We will review budget transfers to determine if actual revenue and expenditures were consistent with the voter approved budget prepared by management. We will review with the Board their practices for monitoring the financial operations of the District and verify that they understand the information that is provided to them. We will also review the financial policies established by the District and verify the District is following those policies. This area was last audited in 2021.
- ◆ Information Technology – Information Technology was identified as an area of higher risk and priority for internal audit consideration due to the relative importance of technology in the District's operations and general cybersecurity risks that currently exist impacting all industries. The internal audit will include social engineering; a review of current policies, access management, system maintenance, logging and monitoring, technology controls and wireless access and network controls; and internal and external vulnerability assessment. This area was last audited (user access audit) in 2024.
- ◆ Purchasing and Cash Disbursements - Due to the financial impact of purchasing and cash disbursements for school districts in general and the volume of activity, this area has been identified as an area of higher risk within the District. We will include selection and testing of cash disbursements from throughout the District to verify that the purchases were reasonable and necessary, were properly approved, and there were available appropriations. We will also verify that all District purchasing policies and internal controls have been followed and that the transaction was supported by appropriate bid or quote information. Since this area is being tested concurrently with the performance of this risk assessment, we do not recommend an internal audit of this area in the near term pending the results of the current internal audit. This area was last audited in 2024.
- ◆ Payroll – Due to the financial impact associated with payroll for school districts in general, the volume of transactions and transition within the department, this area has been identified as an area of higher risk within the District. We will test payroll registers for selected employees to verify that employees listed are employed by the District and are paid in accordance with their contract. We will test hourly employees to verify that the hours paid are supported by time sheets and that the time sheets have been approved by a supervisor and that they have been paid the correct rates. This area was last audited in 2023.
- ◆ Wire Transfers – Due to the inherent risk associated with unauthorized access to the District's assets, this has been identified as an area of higher risk. We will review documentation supporting the wire transfer, verify the transfer was performed by the appropriate person and that funds were transferred to the appropriate party. We will also confirm with all financial institutions with whom the District has a banking relationship with, all individuals who are authorized to initiate and release funds and individuals who have the authority to establish wire transfers to third parties.

BUSINESS RISK ASSESSMENT SIGNIFICANT CHANGES**BUDGETING, GOVERNANCE & REPORTING**

A new Assistant Superintendent of Finance was hired in May 2024, resulting in a change of who is preparing the budget for the District.

SCHOOL LUNCH CASH RECEIPTS

NutriKids is no longer the point of sales system being utilized in the schools. Williamsville CSD transitioned to Mosaic for their point of sales in March of 2024.

FUEL DEPOT

The shop manager has changed from last year's risk assessment, but his job duties remain the same as the prior shop manager. Fuel is now being ordered less frequently as it will be ordered when the level reaches 3,000 gallons rather than 6,000 gallons in prior years.

INFORMATION TECHNOLOGY

There have not been major changes since last year's risk assessment, other than addressing the findings in the prior year's report and strengthening policies and procedures in place at the District. The information technology team is continually working to improve the functionality and processes at the school district. The District has implemented a DR plan, which is being reviewed on an annual basis. The implementation of such plan ensures the District operations can continue in the event of a catastrophe. The District has also implemented Ed Law 2-d compliance training using GCN as well as a service provider to train on cybersecurity. The training includes a series of questions at the end to ensure employees understand the requirements, but does not include pass/ fail testing. Lastly, the District adjusted the Assistant Superintendent of Finance's WinCap rights to read only for all modules except the budget module and administrative user access lockout and password reset modules. Doing so ensures that unnecessary access to financial modules is not permitted.

EMPLOYEE BENEFITS

They are in processes of updating the hiring procedures and manual, with the changes being reflected in the District-wide handbook.

The following business areas did not have significant changes during the review period:

- Budgeting
- STAC Processing
- State Aid
- Medicaid
- Grants
- Centralized cash receipts
- Community education cash receipts
- Payroll
- General ledger maintenance
- Wire and ACH transfers
- Fixed assets

INTERNAL AUDIT PLAN

The Internal Audit Plan summarized below, illustrates the detailed yearly plan estimated to complete the Internal Audit Strategy outlined in the *Business Area Risk Assessment and Internal Audit Strategy* section of this report.

The shaded area denotes the internal audits that were performed during the years 2006 to 2024:

Business Area	Previous	2025	2026	2027
Lines of Business				
<i>Budgeting, Governance, and Reporting</i>	2012, 2021	X		
<i>State Aid</i>	2018			
<i>STAC Processing</i>				
<i>Medicaid Processing</i>				
<i>Grants</i>				
<i>Centralized Cash Receipts</i>	2020			
<i>Community Education cash Receipts</i>				
<i>School Lunch Cash Receipts</i>				
<i>Purchasing and Cash Disbursements</i>	2006, 2019, 2024			
<i>Purchase Cards</i>	2019			
<i>Payroll</i>	2006, 2008, 2014, 2015, 2023			
<i>Health Benefit Trust and Other Employee Benefits</i>	2011			
<i>General Ledger Maintenance</i>	2013			
<i>ACH Transfers</i>	2013		X	
<i>Fixed Assets</i>	2010, 2016			
<i>Fuel Depot</i>	2010			
<i>Student Assessment Security</i>	2014			
Information Technology				
<i>Information Technology</i>	2007, 2018, 2024			X

The above schedule represents the District's three-year internal audit plan based on the risk assessment results identified in this report with only one internal audit performed each year. The District is required to perform a reassessment of risk on an annual basis. The results of the annual reassessment will be the basis for identifying internal audit priorities and determining the internal audit plan in future years.

APPENDIX - RISK CATEGORY DEFINITIONS

INHERENT RISKS

EXTERNAL/MARKET REPUTATION

Negative Publicity – The risk of public disclosure of operations will negatively influence public perception that impacts the District's ability to pass a budget and meet its strategic objectives.

FINANCIAL

Achieving Financial Goals – The risk that the District will be unable to meet their financial goals and be pressured by the Board or management to take unwise or inappropriate actions to report results which meet market expectations.

Materiality – The risk that any financial reporting activity will misrepresent results by an amount that would reasonably change voter or other external third party assessments of the District's performance.

Volatility – The risk that financial reporting will be inaccurate, incomplete or untimely.

Use of Significant Estimates – The risk that financial reporting activity will misrepresent actual business results due to heavy reliance on estimates, accruals, adjustments or reserves that are subjective and difficult to accurately quantify and/or associate with the occurrence of business events.

OPERATIONAL

Inefficient/Ineffective Internal Controls – The risk of inadequate or poorly designed internal controls and accountability.

Employee Error – The risk of unintentional errors by employees due to a lack of competence or training or unfamiliarity with policies and procedures.

Inappropriate Data Usage – The risk of the misuse of sensitive or confidential information by employees or other outside parties.

Non-Routine/Complex Transactions – The risk that incorrect or inconsistent handling of infrequent or complex activities could cause inconsistent financial reporting.

Compliance with Policies and Procedures – The risk that staff responsible for executing business activities will fail to comply with the District's policies and procedures, whether due to lack of training, failures of communication or mindful disregard.

LEGAL/REGULATORY

Legal and Economic Impacts – The risk of direct or indirect impact on activities from changes in the regulatory environment.

Unresponsive to Legal/Regulatory/Compliance Changes – The risk that the District is unaware of or does not respond to changes in laws and regulations to ensure compliance.

Litigation Issues – Lawsuits can result in expensive settlements, litigation costs and corrective action (e.g. employee/customer litigation, contract/fiduciary liability, etc.).

STRATEGIC

Insufficient or Inadequate Strategic Planning – The risk that an inefficient and ineffective strategic planning process, including poor assumptions, results in the District's inability to meet their goals and objectives.

Lack of Appropriate Governance – The risk that senior management or Board members commit actions that are detrimental to voter's' interests, including misrepresenting the District's intentions or business results.

People or Key Resources – The risk that barriers (e.g. high turnover, inexperienced staff/skill limitations, excessive reliance on a key staff member, insufficient staffing/resources, etc.) can increase business risk impact and likelihood of its occurrence.

Organization Reputation – The risk that the District's reputation could be exposed based on lack of voter satisfaction with services, or ability to provide new and innovative educational programs; negative public reaction due to identified regulatory, compliance or legal issues.

TECHNOLOGY/SYSTEMS

Lack of Information Integrity – The risks associated with the authorization, completeness, timeliness and accuracy of transactions/data as they are entered into, processed and reported by various systems.

Lack of Timely, Reliable, and Relevant Information for Decision Making – The risk that relevant internal and external information necessary for decision making is not available on a timely basis and/or is unreliable.

Inadequate Data Security and Access – The risk of not adequately restricting access to and protecting information.

Sensitivity of Data – The risk that the District will divulge, inappropriately use or fail to control student or employee data which is confidential or private.

PEOPLE/CULTURE

Lack of Clear Roles and Responsibilities – The risk that roles and responsibilities are not clearly defined, communicated, and understood by employees.

Deficient Values, Integrity, and Ethics – The risk of an employee breach of District values and Code of Conduct standards related to integrity, ethics and discrimination.

Inappropriate Performance Incentives – The risk of either insufficient performance incentives or incentives that are unrealistic or misunderstood causing employees to act in an inappropriate manner.

FRAUD

Misappropriation of Assets – The risk that the District engages in external and/or internal schemes, such as embezzlement, payroll fraud and theft.

Misconduct/Abuse – The risk that transactions or activities could be susceptible to management override (e.g. conflicts of interest, code of ethics violations, etc.). District could be directly or indirectly involved in monitoring and identifying misconduct and/or abuse.

External Crime – The risk that activities could be exposed to external theft and destruction (e.g. robbery, asset/information theft, etc.). District could be directly or indirectly involved in monitoring and identifying external crime.

External Fraud – The risk that transactions and activities could be exposed to external fraud (e.g. check frauds and kiting). District could be directly or indirectly involved monitoring and identifying external fraud.

COSO CONTROL RISKS

Monitoring – This category includes identifying a mechanism or process to assess internal controls on an ongoing basis to ensure that changes are incorporated effectively.

Information and Communication – This category includes the assessment of the technology environment and includes an assessment of the reporting internally and externally. The internal communication to manage the business on a daily basis is assessed to determine the effectiveness and reliability of the financial information that is used.

Control Activities – These controls are at the process level and include preventive and detective controls. The assessment for control activities requires a selection of key processes and a review of the transaction flow to identify and test the critical controls to determine the effectiveness.

Risk Assessment – These controls are the overall management and strategic planning methods that are in place. The process for strategic planning for the District and each department and how the plan is executed during the year is the subject of this review. Material changes in the legislation or regulations and the process that management performs to execute a transaction will be assessed.

Control Environment – The controls in this category include integrity/ethical values, code of conduct, disciplinary action, structure of organization, involvement of the Board of Education, human resources and other actions that control the tone of the organization.