Frontier Central School District

Risk Assessment, Recommendations and Findings for 2024 - 2025

Frontier Central School District
Risk Assessment,
Recommendations and Findings
for 2024 - 2025

Table of Contents

To the Audit Committee of the Board of Education
of the Frontier Central School District

We are pleased to report on the Internal Control procedures specific to the Information
Technology ("IT"), Purchasing and Accounts Payable ("AP"), and Athletics ("A") processes of
the Frontier Central School District (the "District"). We tested the IT, AP, and A processes at the
direction of the Board of Education (the "Board") as a result of our Risk Assessment Report dated
January 31, 2025. The purpose of our engagement is to provide recommendations to strengthen
controls and reduce the identified risks. This report was developed from inquiry, observations and
tests of internal control.

The District's risks are the risks that an action or event will adversely affect its ability to successfully
achieve its objectives. The Risk Assessment section of the report analyzes the findings that were
identified during our engagement.

For purposes of this report, internal control is a process affected by the Board, department heads
and other personnel, designed to provide reasonable assurance regarding the achievement of
objectives in the reliability of financial reporting and safeguarding of assets. We have evaluated
the District's current internal controls specific to the IT, AP, and A processes and have provided
our risk assessment and recommendations for strengthening controls and reducing identified risks.

As noted, the purpose of our engagement was to assist you in improving the internal controls and
reducing the risks that face the District. However, it is ultimately your responsibility to assess the
adequacy of your risk management system. In performing our engagement, we relied on the
accuracy and reliability of information provided by District personnel. We have not audited,
examined, or reviewed the information, and express no assurance thereon.

The accompanying comments and recommendations are intended solely for the information and use
of the Audit Committee, the Board, department heads and others within the District and should not
be used for any other purpose.

We appreciate the opportunity to serve you and thank the individuals in your District for their
cooperation. We have already discussed many of these comments and suggestions with various
District personnel, and we will be pleased to discuss them in further detail at your convenience.
Through our ongoing involvement with you as a client and our knowledge of your processes, we
would be pleased to perform any additional studies of these matters or to assist you in implementing
the recommendations.

Tronconi Segarra & Associates LLP

Williamsville, New York
March 11, 2025

Risk Assessment

Frontier Central School District

Risk Assessment

Overview

The Frontier Central School District's (the "District") risks are the risks that an action or event will adversely affect the District's ability to successfully achieve its objectives. During our engagement, we became aware of various sources of risk that impact the District. We evaluated these risks by using two distinct assessments of impact and likelihood. A simple rating scale has been developed for this purpose. The rating scale ranges from minor to significant impact, and low to high likelihood, using a 3-point scale.

Impact refers to the extent of the consequences or implications if the risk does occur. To assess impact, we have determined how much of an impact the risk has if it does occur:

- A minor impact suggests that the risk would not have important implications to the District.

- A moderate impact suggests that the risk could have implications for the District's ability to succeed.

- A significant impact suggests that the risk would have important implications to the District.

Likelihood refers to the probability that the risk may occur given the current context of the District. To assess likelihood, we have determined how likely it is that the risk will occur in the future, given what is currently done to manage said risk:

- A low likelihood suggests that the risk is unlikely to occur, given its nature and current risk management practices in place.

- A medium likelihood of occurrence suggests that the risk has a moderate probability of occurrence.

- A high likelihood of occurrence suggests that the risk is likely to occur, despite the current risk management practices in place.

The Risk Management Tolerance Model and the Risk Assessment Matrix that follow summarizes these risks and assesses their impact and likelihood. Cycles plotted in the yellow sections of the matrix are considered to have moderate risk, are considered to be important, and should be given reasonable priority. Cycles plotted in the green section of the model are considered least risky and remediation efforts to address deficiencies in these cycles would be expected to be addressed during routine operations of the District.
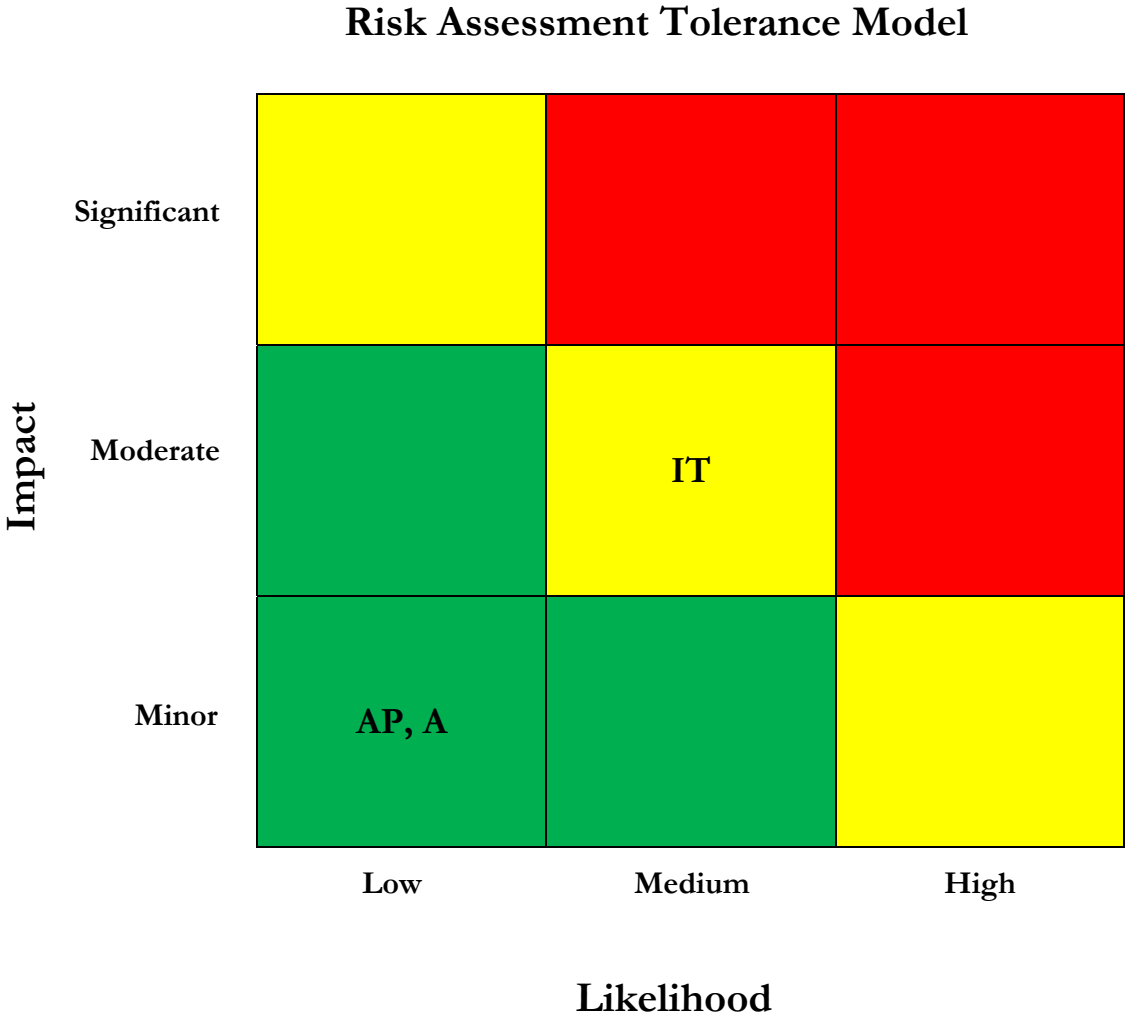
Overview (continued)

We have developed the risk assessment around significant financial transaction cycles as a means by which the associated risks can be easily understood and managed. The Internal Control Recommendations section of this report presents recommendations with more detailed information regarding criticality and implementation timelines. In accordance with the 2024- 2025 Internal Audit Plan, the significant cycles or areas in which we have performed testing are as follows:

- Information Technology (IT)
- Purchasing and Accounts Payable (AP)
- Athletics (A)

Risk Assessment Tolerance Model

Impact	Low	Medium	High
Significant	🟨	🟥	🟥
Moderate	🟩	🟨 IT	🟥
Minor	🟩 AP, A	🟩	🟨

Likelihood

Risk Assessment Matrix

Cycle	Risk Assessment Based on Procedures Performed	Impact	Likelihood
IT	We noted moderate overall risk in the Information Technology cycle. We identified five recommendations for improvement: three which we consider to be important to District operations and one which we consider to be urgent and should be addressed as soon as possible.	**Moderate**	**Medium**
AP	We noted minor overall risk in the Purchasing and Accounts Payable cycle. We identified one recommendation for improvement which can be addressed during routine operations of the District.	**Minor**	**Low**
A	We noted minor overall risk in the Athletics cycle. We identified three recommendations for improvement which can be addressed during routine operations of the District.	**Minor**	**Low**

Internal Control Recommendations

Frontier Central School District

Internal Control Recommendations

Overview

Internal control recommendations represent those areas that afford department heads of the District the opportunity to improve financial reporting and internal controls, to better safeguard District assets and/or to more efficiently or accurately record, summarize and report financial transactions and information. They also represent those areas that may improve efficiency of operations and accounting functions, potentially resulting in cost savings.

We have provided a criticality rating and an implementation timeline for each internal control recommendation. Criticality ratings considered included urgent, important and routine. The implementation timelines considered were short-term and long-term, reflecting the effort and time required to implement the applicable recommendation while factoring in the criticality assigned thereto. Short-term refers to a finding that we believe can be corrected within one year. Long-term refers to a finding that may require changes to the systems and/or procedures of the District that may require over one year to effectuate change.

As a result of the procedures we performed, we identified nine (9) total recommendations. The criticality and timeline for the recommendations within the respective cycles that we tested are as follows:

Internal Control Area	Number of Recommendations	Criticality			Timeline	
		Routine	Important	Urgent	Short-Term	Long-Term
Information Technology (IT)	5	1	3	1	5	0
Purchasing & Accounts Payable (AP)	1	1	0	0	1	0
Athletics (A)	3	1	2	0	3	0
Total Recommendations	9	3	5	1	9	0

INFORMATION TECHNOLOGY (IT)

RECOMMENDATION 1 –

Criticality: Important
Timeline: Short-Term

Finding: While the District has adopted policies relating to Information Technology ("IT"), several policies have not been reviewed or updated for several years, and, as a result, may not reflect the District's actual policies and procedures currently in place or the most up to date guidance on IT best practices for school districts.

Background: The District has adopted several policies relating to Information Technology. We reviewed nine of these policies and found that, while the policies cover most of the important aspects of the District's IT environment, eight of the nine policies reviewed have not been updated within the last four years. Certain policies have not been updated since as far back as 2013, such as the policy relating to student use of computerized information resources and internet safety and content filtering. The most up-to-date document was the Student Use of Technology Agreement, which was dated as of the 2024-25 fiscal year.

Rationale –

Impact*: Moderate* – While there are policies in place over IT procedures for the District, there is a risk that they do not fully encompass current best practices or District procedures, due to being outdated. Because the nature of IT controls and security is constantly evolving, the risk of outdated policies exposing the District to risk could have, at the least, a moderate impact on the District.

Likelihood*: Medium* – As a result of the outdated policies, there is an increased likelihood that the policies will not cover all key situations that may arise with regards to the District's IT environment. Also, because of the constantly evolving nature of IT and the threats surrounding IT, there is a medium likelihood of the above identified risks occurring.

Recommendation: We recommend that the District ensure that all policies relating to the District's IT environment are regularly reviewed and updated, as necessary, to remain relevant with the District's practices and industry best practices in this process area.

RECOMMENDATION 2 –

Criticality: Urgent
Timeline: Short-Term

Finding: The District does not maintain cybersecurity insurance.

Background: School districts are increasingly reliant on technology for administrative operations, student learning, and communication. Districts have also become a prime target of ransomware attacks throughout the country. Cybersecurity insurance provides the District with certain financial protections against attackers, including certain policies that include risk management strategy, and may cover the ransom fees and assist with replacing and repairing the IT network. Additionally, cybersecurity insurance was included as a component of the incident response plan recently developed for the District by an outside consultant.

Rationale -

Impact*: Significant* – By not having cybersecurity insurance in place, the District is at a significant risk that a ransomware attack could severely impact District operations, both with regards to the District's IT environment and the District's financial condition.

Likelihood*: High* – With the ever-increasing ransomware attacks focused on school districts, the likelihood of the District's lack of cybersecurity insurance significantly impacting its operations is high.

Recommendation: We recommend the District investigate, obtain quotes for, and purchase cybersecurity insurance for further safeguarding of the District's technology infrastructure and sensitive data.

RECOMMENDATION 3 –

Criticality: Important
Timeline: Short-Term

Finding: The Technology Department is not always able to fully disable network user accounts when an employee no longer works for the District or needs to be restricted from email or network access. We identified 145 user accounts that were not disabled in a timely manner.

Background: The Technology Department has established a scripting procedure that integrates with the District's financial software (nVision) and creates new user accounts when a new employee is added to nVision and disables user accounts when an employee is removed from nVision. There are certain instances, however, when an employee user account needs to be disabled but the employee cannot be removed from nVision. When this occurs, the Technology Department will change the user account to a different organizational unit that restricts the employees' access to the network.

Rationale –

Impact: *Moderate* – The impact of not updating access or disabling employee user accounts in a timely manner could have a moderate impact on the District as these accounts serve as entry points to the District's network that could be accessed by malicious users.

Likelihood: *Medium* – The likelihood of inappropriate access to the District's network through an employee account that was not updated or disabled in a timely manner is assessed as medium given the potential access such accounts may have to the District's network and data, and the inherent risk that malicious users will attempt to access network accounts.

Recommendation: We recommend that, when a user account is no longer needed, that the network account be disabled or appropriately restricted in a timely manner to reduce the risk of unauthorized access to the account.

RECOMMENDATION 4 –

Criticality: Important
Timeline: Short-Term

Finding: We found that between 34 and 42 percent of District IT users did not complete the monthly security awareness training sent out by the Technology Department during the 2024-25 school year, for the months of October 2024 through December 2024.

Background: Security awareness training is provided on an annual basis to all staff. Additionally, the Director of Technology sends out short, monthly security awareness training videos to all staff members on relevant cybersecurity topics. The Technology Department has a goal of 85 percent completion for these monthly training sessions.

Rationale -

Impact: *Moderate* – As a result of District network users not participating in monthly security awareness trainings, there could be a moderate impact on the District as technology is an integral part of the District's day-to-day operations, and user error and inadequate awareness is a common cause of IT network breaches.

Likelihood: *Medium* – The likelihood of a lack of user participation in monthly security awareness training having an impact on the District is assessed as medium as District users are constantly interacting with the District's IT environment.

Recommendation: We recommend that the Technology Department continue to provide monthly security awareness training, and that District administrators assist in stressing the importance of user participation in the monthly training sessions in order to increase District-wide participation.

RECOMMENDATION 5 –

Criticality: Routine
Timeline: Short-Term

Finding: The District does not have a clear, written policy or procedure around the use of help desk tickets with the Technology Department which would identify the types of IT issues or situations that would require the submission of a help desk ticket.

Background: While the District has a help desk ticketing system in place, the Director of Technology indicated that tickets are typically submitted for smaller issues such as password resets, software installation requests, device troubleshooting, network connectivity problems, and access issues. However, District staff typically will not submit help desk tickets for larger problems that require intervention, such as system outages, security concerns, hardware failures, software malfunctions, or account access requests.

Rationale -

Impact: *Moderate* – By not having documented policies and procedures for events that require help desk tickets for IT issues or situations that require intervention, the Technology Department may not become aware of significant hardware, security, or other issues with the District's IT environment, which could have a moderate impact on the District's operations, due to the District's reliance on its technology system and network for its operations.

Likelihood: *Medium* – The likelihood of a lack of policies and procedures around help desk ticketing for the District's IT environment having an impact on the District is assessed as medium, as without a consistent process for help desk ticketing in the event of an IT issue, the Technology Department will not be able to timely resolve issues as they arise.

Recommendation: We recommend that the District adopt a written policy and procedure, and enforce such procedure, regarding the use of IT help desk tickets, including when tickets must be submitted and by whom.

PURCHASING AND ACCOUNTS PAYABLE (AP)

RECOMMENDATION 1 –

Criticality: Routine
Timeline: Short-Term

Finding: While the District has adopted policies relating to the purchasing and accounts payable processes, several policies have not been reviewed or updated for several years, and, as a result, may not reflect the District's actual policies and procedures currently in place or the most up to date guidance on purchasing and accounts payable best practices for school districts. Additionally, there may be opportunities to eliminate policies with duplicate information.

Background: The District has adopted several policies relating to purchasing and accounts payable. We reviewed ten of these policies and found that, while the policies cover all appropriate aspects of the purchasing and accounts payable processes, each of the policies reviewed has not been updated in the last several years. Certain policies have not been updated since as far back as 2004, such as the policy relating to obtaining authorization for purchasing requests. The most recent policy update occurred in 2022, relating to District credit card use.

Rationale -

Impact*: Minor* – While there are policies in place over purchasing and accounts payable procedures, there is a risk that they do not fully encompass current best practices or District procedures, due to being outdated. Additionally, the recent turnover within the Business Office may affect the efficient operation of the purchasing and accounts payable procedures.

Likelihood: Low – As a result of the outdated policies, combined with the recent turnover in the Business Office, there is a likelihood that the policies will not cover all key situations that may arise during the District's purchasing and account payable processes. However, there are multiple employees within the Business Office who demonstrated adequate experience with regards to purchasing and accounts payable through their work with school districts in general, which reduces the likelihood of occurrence to a low level.

Recommendation: We recommend that the District ensures that all policies relating to purchasing and accounts payable are regularly reviewed and updated, as necessary, to remain relevant with the District's practices in this process area.

ATHLETICS (A)

RECOMMENDATION 1 –

Criticality: Routine
Timeline: Short-Term

Finding: Inventory listing forms completed for each sports team and coach did not include the dates when equipment and uniforms were issued and returned and were not signed by the Athletics Director when the equipment was issued or returned.

Background: At the beginning and end of each season, the Athletics Director and individual coaches will complete an inventory listing form, which details out the equipment and uniforms that were issued to the coach for their respective sports team. These forms must be completed before stipend payments to coaches are approved.

Rationale -

Impact*: Minor* – Ensuring proper dates and signatures of both the coach and Athletics Director are included on inventory listing forms for each sports team in the District is important for ensuring that all inventory is properly accounted for when issued and returned. While the forms reviewed did not include the issued or return dates, or the Athletics Director's signature, the forms were still sufficiently detailed and signed by the coach to document the inventory received and returned, reducing this risk to a minor impact.

Likelihood*: Low* – As the payment of a coach's stipend is dependent on the complete, accurate, and timely return of issued equipment and uniforms, the likelihood of the risks mentioned above occurring is low.

Recommendation: We recommend that the Athletics Director note the date that inventory was issued to and returned by the respective coaches, and that the Athletics Director signs the inventory form when items are issued and returned.

RECOMMENDATION 2 –

Criticality: Important
Timeline: Short-Term

Finding: We noted that, while an inventory spreadsheet of equipment and uniforms on hand was provided during our fieldwork, such a file is not typically completed or available. Additionally, the inventory spreadsheet provided did not include key information about the items, including where the inventory was maintained, who had custody of the inventory or the cost of the items.

Background: The Athletics Director provided a general inventory spreadsheet that documented the uniforms and equipment on hand for each sports team within the District. However, we noted during our walkthrough with the Athletics Director that this inventory record for all equipment and uniforms was only created as a result of our documentation request and is not currently maintained by the department.

Rationale -

Impact*: Moderate* – As a full inventory record of Athletics department equipment and uniforms is not regularly maintained and updated with all pertinent information, such as location, custody holder and cost, there is a moderate risk that inventory may be lost, misplaced, or misused.

Likelihood*: Low* – While the lack of inventory records would have a moderate impact on the operations of the District's Athletics department, there is a low likelihood of the above-mentioned risks occurring, due to the inventory listing forms created and maintained for each team's season with the respective coaches.

Recommendation: We recommend that the Athletics Director create and regularly maintain a full inventory spreadsheet, noting the equipment and uniforms on hand for each sports team, the location where the inventory is maintained, the individuals who have custody of said equipment and uniforms, and the cost of the items.

RECOMMENDATION 3 –

Criticality: Important
Timeline: Short-Term

Finding: While a key distribution report is maintained, showing all keys that have been issued to District coaches for access to storage areas and athletics facilities, the report does not appear to be consistently updated when keys are returned at the end of a season or when an employee separates from District employment.

Background: We noted that, of the twenty-nine coaches who were issued keys for various athletics facilities, there were fifteen coaches in total who have had keys issued to them since 2022 or 2023 that have not yet returned the keys. Of these fifteen, ten were full-time District employees, four were only hired as coaches for the District, and one was a coach who is no longer employed by the District.

Rationale -

Impact*: Moderate* – Due to the key distribution report not being regularly updated with the date that keys are returned, there is a moderate risk that keys may be lost, misplaced, or misused.

Likelihood*: Low* – While the incomplete key distribution report could have a moderate impact on the operations of the District's Athletics department, there is a low likelihood of the above-mentioned risks occurring. The Athletics Director is aware of the location of keys and requires coaches that are not full-time District employees to return their issued keys prior to receiving their coaching stipend.

Recommendation: We recommend that the Athletics Director ensure that the key distribution spreadsheet is regularly updated when coaches return keys at the end of a season or when they separate from District employment or service as a coach.