Buffalo City School District

Risk Assessment – Information Technology Cycle
Findings and Recommendations
For the Year Ended June 30, 2016
with Updates and Responses through June 30, 2018

Buffalo City School District

Risk Assessment – Information Technology Cycle
Findings and Recommendations
For the Year Ended June 30, 2016
with Updates and Responses through June 30, 2018

Table of Contents

TRONCONI SEGARRA & ASSOCIATES LLP
Certified Public Accountants
Business Consultants

To the Audit Advisory Committee of the Board of Education
of the Buffalo City School District
Buffalo, New York

We are pleased to report on the risk assessment for the information technology cycle of the Buffalo City School District (the "District"). The purpose of our engagement is to assist you in the development of a risk assessment of District operations, and provide recommendations to strengthen controls and reduce the identified risks. This report was developed from inquiry, observations and tests of internal controls performed during the 2015-2016 fiscal year with updates and responses through June 30, 2018.

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

For purposes of this report, internal control is a process, affected by the Board of Education (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 and have provided our risk assessment and a set of 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 your 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 Advisory Committee, the Board of Education, 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

January 22, 2019

Risk Assessment – Information Technology Cycle

Buffalo City School District

Risk Assessment – Information Technology Cycle
For the Year Ended June 30, 2016
with Updates and Responses through June 30, 2018

Overview and Scope

The District's 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 on 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 on the District.

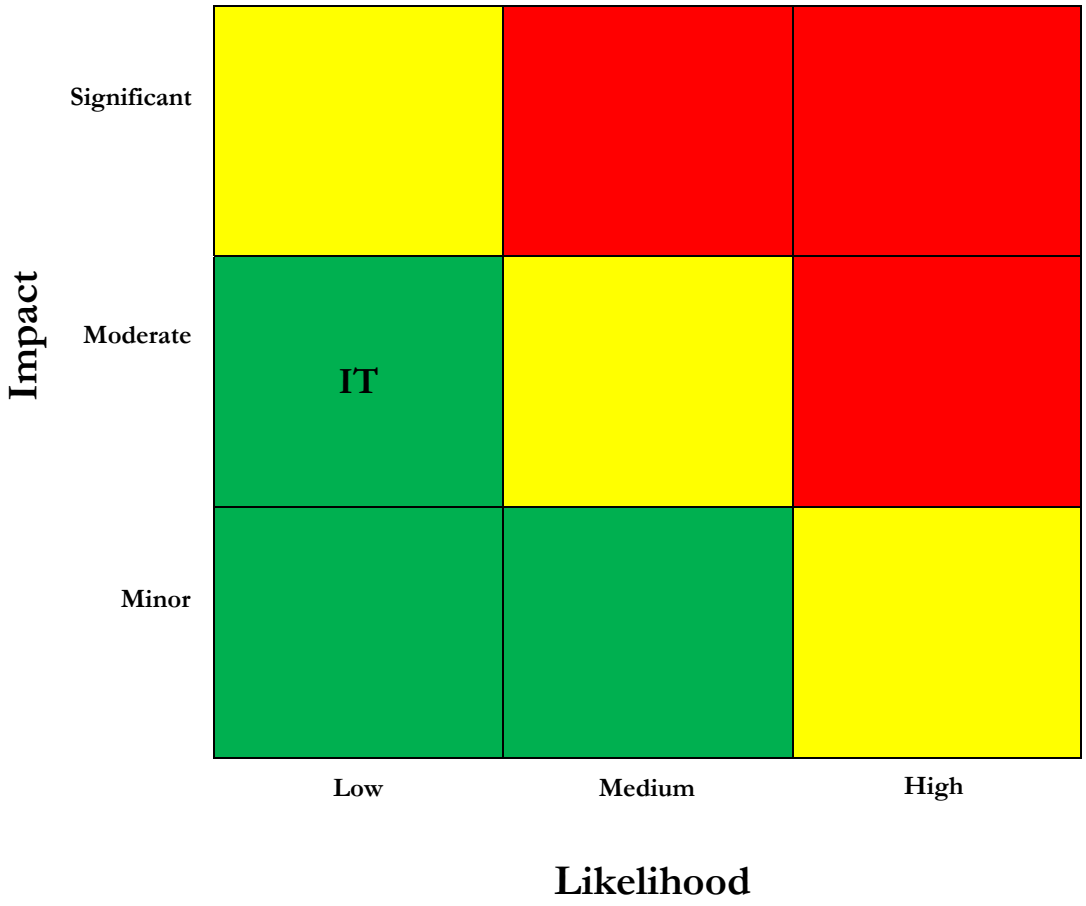
Likelihood refers to the probability that the risk may occur given the current context of the District. To assess likelihood, we have determined how likely it is that the risk will occur in the future, given what is currently done to manage said risk:

- 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 summarize these risks and assess their impact and likelihood.

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 detail information regarding criticality and implementation timeliness. This report includes our work on the information technology cycle.

Risk Management Tolerance Model



Risk Assessment Matrix

Cycle	Risk Assessment Based on Procedures Performed	Impact	Likelihood
IT	We noted moderate overall risk in the Information Technology cycle. Risks identified related to the lack of comprehensive IT Security Plan and Disaster Recovery Plan, improper documentation for new users, and a lack of proper lockout procedures.	**Moderate**	**Low**

Summary of Internal Control Recommendations – Information Technology Cycle

Buffalo City School District

Summary of Internal Control Recommendations – Information Technology Cycle
For the Year Ended June 30, 2016
with Updates and Responses through June 30, 2018

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 costs savings.

We have provided a criticality rating and an implementation timeline for each internal control recommendation. Criticality ratings considered were 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.

As a result of our procedures performed for the information technology cycle, there were three (3) total recommendations. The criticality and timeline for the recommendations is as follows:

		Criticality			Timeline	
Internal Control Area	Number of Recommendations	Routine	Important	Urgent	Short-Term	Long-Term
Information Technology (IT)						
Information Technology Department	3	0	3	0	1	2
Total Recommendations	3	0	3	0	1	2

Timeline – Each of the detail findings includes a timeline reference of either "short-term" or "long-term." Short-term refers to findings that we believe can be corrected within one year. Long-term refers to findings that necessitate changes to organization, systems, or procedures that may require over one year to effectuate the change.

Detail Findings and Recommendations – Information Technology Cycle

RECOMMENDATION #IT1 — IT Framework

Criticality: **Important**
Timeline: **Long-Term**

We noted that the District does not have a comprehensive written Information Technology security plan. Without the IT security plan, there is the risk that the District does not formally identify threats to its IT environment, the ways the District will deal with these threats and how the District will respond to breaches if they occur.

We recommend that the District prepare and publish a comprehensive IT security plan and provide a copy of the plan to the appropriate users. Also, the IT security plan should be tested and reevaluated on a periodic basis.

Board Response:

The District has neither a comprehensive written Information Technology security plan, nor the internal expertise to create one. While some steps have been taken to address cyber security-related issues, a full audit from a cyber security firm is necessary to identify the full scope of the problem and create an actionable plan to address those concerns. Without external support on best practices for cyber security, the full scope of the problem may not be realized, potentially placing the District at risk for a cyber-attack.

Further, IT budgeted for and is currently working with HR on filling a new position specifically to address Cyber Security.

In parallel with seeking out external expertise, over the course of the last year, we have implemented the following steps towards an end goal of a comprehensive security plan:

- Engagement with Microsoft and implementation of a centrally managed antivirus and endpoint protection software.
- Enterprise-level encryption software has been implemented on administrative laptops.
- The firewall has Intrusion Detection Systems (IDS) fully implemented for external threats, and the firewall logs are analyzed for potential anomalies.
- BPS has had an initial engagement with an industry expert to analyze current needs and craft District policy.
- Implementation of an identify management platform.

Moving into 2018, we are taking the following next steps to develop and implement a comprehensive IT security plan:

- Security "POP SLAM" scheduled with Microsoft to analyze account rights and user directory permissions.
- Continued engagement with the security vendor to produce a testable security plan.
- Secure in-house expertise through the hiring of a cybersecurity expert.

RECOMMENDATION #IT2 — User Accounts

Criticality: Important
Timeline: Short-Term

We noted for a sample of users that there is no signed confidentiality agreement for IEPDirect Users. Prior to a user being granted access to IEPDirect.com, he or she must sign an IEPDirect.com Confidentiality and Non-Disclosure Agreement. During our testing of 15 IEPDirect.com users, we noted the District could not provide signed Confidentiality and Non-Disclosure Agreements for 2 of the 15 users tested.

We recommend the Special Education Department maintain all signed IEPDirect.com Confidentiality and Non-Disclosure Agreements.

Board Response:

IEP Direct falls under the management of the Special Education Department, and is not hosted internally. With that in mind, developing, distributing, and collecting Confidentiality and Non-Disclosure agreements for IEP Direct is the responsibility of the Special Education Department.

Identifying the best method to execute these tasks for IEP Direct and similar applications will be addressed through the department's cyber security audit. In the meantime, we will reach out to the Special Education Department alerting them of this problem.

RECOMMENDATION #IT3 — User Accounts

Criticality: Important
Timeline: Long-Term

We noted that the District does not require users to lock their computers before stepping away from the computer for an extended period of time. During our fieldwork, we observed that a user remained logged into their computer even though they had been away from their desk for over an hour. The computer's screen saver is initiated, but the computer did not lock after an extended period of idleness.

We recommend the District publish a policy to require users to lock their computers if they are expected to be away from their computer. The District could also consider implementing automatic locking after a predefined period of inactivity. We acknowledge that the lockout policy implemented for administrative staff may be different than the policy for instructional staff due to practical constraints.

Board Response:

While there is currently no District policy in place to require users to log-off of a machine if they are away from their computer, we have implemented lock screens for administrative machines. Further study will be needed to assess and address the required balance between instructional needs and security. For example, computers connected to interactive whiteboards are left on and unlocked while teachers are navigating through the classroom working with students.

As part of a cyber-security audit, the IT Department will seek out best practices to develop and propose to the Board of Education a log-off policy. In conjunction, the IT Department will test the functionality of using screen savers as lock screens for all users.