Prepared by Toski & Co., P.C.

TOSKI & CO., P.C.

6390 Main Street, Suite 200 • Williamsville, NY 14221 • Ph: (716) 634-0700 • Fax: (716) 634-0764

Visit us at www.ToskiCPA.com

Control Cycle Audit of

Information Technology

BLIND BROOK-RYE
UNION FREE SCHOOL DISTRICT

Blind Brook-Rye Union Free School District
390 North Ridge Street
Rye Brook, NY 10573

July 7, 2015

TOSKI & CO., P.C.
CERTIFIED PUBLIC ACCOUNTANTS

To the Audit Committee
Blind Brook-Rye School District
Rye Brook, New York

We have performed a review of the internal controls of the Information Technology function. We obtained an understanding of these internal controls by inquiry, observation and the inspection of documents and records. Our review of the Information Technology Area included examining all written policies and procedures as well as a list of current hardware and software utilized. Particular attention was given to issues such as user IDs and passwords; data and application access/permissions; physical safeguards; routine data backup; and disaster recovery planning.

We conducted our review in accordance with attestation standards established by the American Institute of Certified Public Accountants. Such standards require that we understand the School District's management controls and compliance with those laws, rules and regulations that are relevant to the District's operations that are included in our scope. A review includes examining, on a test basis, evidence that supports the transactions performed within the Information Technology area. We believe our review provides a reasonable basis for our findings, conclusions and recommendations included in this report.

The vulnerabilities and sensitivity of the information identified in our audit should preclude this report from being part of the public domain. If a copy is requested or made public, a redacted version should be considered.

Toski & Co., CPAs, P.C.

TOSKI & CO., P.C.
Rochester, New York

6390 Main Street, Suite 200 | Williamsville, New York 14221 | P 716.634.0700 | TF 800.546.7556 | F 716.634.0764 | **ToskiCPA.com**

BACKGROUND:

The Blind Brook-Rye Union Free School District (District) is located in Westchester County and has a total enrollment of approximately 1,600 students combined for the high school, middle school and elementary schools. The District utilizes five educational buildings, a transportation building, and a maintenance building for all students, faculty and other support staff.

OBJECTIVE:

The objective of our audit was to evaluate the internal controls over the Information Technology function at the Blind Brook-Rye Union Free School District.

AUDIT SCOPE, PROCEDURES AND FINDINGS:

Our overall goal was to assess the adequacy of the internal controls put in place by officials to safeguard the assets of the Blind Brook-Rye Union Free School District. To accomplish this, we performed a risk assessment of the District's internal controls so we could evaluate the risk within each control cycle. Our risk assessment evaluated the following areas: Budgeting; Cash Receipts and Revenue; Transportation; Food Service; Extra-Classroom Activity Fund; Capital Assets/Projects and Indebtedness; Purchasing, Claims, Accounts Payable and Cash Disbursements; Payroll and Personnel; and Accounting, Reporting and Information Technology. Based on prior audit findings and concerns of the District, the Audit Committee of the District selected to review Information Technology. As a result, our testing was limited to this area.

In performing our review of the Technology function, our scope was limited to July 1, 2014 through April 30, 2015.

AUDIT SCOPE, PROCEDURES AND FINDINGS *(Continued):*

Information Technology

Information Technology Policies, Procedures and Physical Access

- Review the District's Policies and Procedures related to Information Technology.
- Review the Technology organizational chart to evaluate staffing levels and functional responsibilities.
- Examine the server rooms and technology closets to determine that security over physical access is adequate.
- Determine whether the server rooms are equipped with dedicated air conditioning.
- Determine whether the server rooms are equipped with fire detection and suppression capabilities.
- Determine whether there is a system to provide automated notifications to alert technology staff in the event of potentially damaging conditions in the server rooms, such as loss of air conditioning or power.
- Verify there are sources for backup power in place for the servers, such as Uninterrupted Power Supply (UPS) devices and backup generators.
- Verify that a physical inventory of all technology equipment is maintained and periodically verified.
- Determine whether procedures are adequate to properly identify and dispose of technology hardware, ensuring that all critical or confidential data has been removed.

AUDIT SCOPE, PROCEDURES AND FINDINGS *(Continued):*

Information Technology Policies, Procedures and Physical Access (*Continued*)

FINDINGS:

The controls over Information Technology Policies and Procedures and Physical Access are operating effectively with the following exceptions noted:

1. The server room stores the core of the District's information technology infrastructure and is critically important to the performance of the financial systems and other key operating systems related to communications, security, and student information. We noted that the server rooms, in both the Ridge Street and High School locations, are not equipped with smoke detectors. The lack of these alarms makes it more likely that a potential fire would result in catastrophic damage and severely impact the District's infrastructure. Additionally, the fire extinguisher in the Ridge Street server room has not been inspected since December 2013.

2. Access to the server rooms is controlled by key rather than a badge swipe system, which offers stronger controls and greater flexibility in restricting access. The District does, however, have video surveillance of the Ridge Street server room to help monitor access.

3. The District does not have backup generators at either the Ridge Street or High School locations that could supply power to the server rooms in the event of a power outage. The UPS devices begin to power the servers when the main power supply is lost, but can only do so for a very limited period of time. The UPS devices are not currently configured to perform a gradual shut down of the servers when there is a loss of power. Consequently, when their batteries are depleted and ultimately fail, the servers will experience an abrupt power loss which could damage the District's hardware and/or data.

4. During our review of server room hardware, we noted that the District's financial software (Finance Manager) is operated using an outdated server. This server is running Windows 2003, an operating system no longer supported by Microsoft. In the event this hardware fails, this could potentially cause compatibility issues or other complications when transitioning the software and data to a new device.

5. During our review of server room hardware, we noted that one of the UPS devices in the High School server room was not operating optimally and would likely not have sufficient power to support the full load of the server it was connected to in the event of a power failure.

6. During our review of hardware located in the technology wiring closets, we noted that janitorial supplies were in contact with fiber cables and other wiring connected to hardware. This wiring and/or hardware could potentially be dislodged or otherwise damaged when the janitorial supplies are accessed.

AUDIT SCOPE, PROCEDURES AND FINDINGS *(Continued):*

Information Technology Policies, Procedures and Physical Access (*Continued*)

RECOMMENDATIONS:

1. We suggest the District take appropriate action to install smoke detectors and/or fire alarms inside the server rooms. These alarms should be integrated into the District's alarm systems so that the proper authorities and staff/management are immediately informed when an alarm is indicated. Ideally, server rooms should also be equipped with a fire suppression system to minimize any damage caused by a fire. However, these systems are often very expensive and may not be deemed practical given budget considerations. At a minimum, fire extinguishers should be installed in the server room and technology closets. Fire extinguishers should be inspected on a regular basis.

2. We suggest the District consider installing a badge swipe system to control access to the server rooms. This type of system could improve the District's ability to control access and would provide a permanent record of who is accessing the servers and when.

3. We recommend the District consider installing backup generators at the Ridge Street and High School locations that would support the server rooms in the event of a main power failure. If this is not feasible due to cost considerations, the District should configure the UPS devices to begin a gradual shutdown of the servers when there is a main power failure. This precaution would protect the District's hardware and data by ensuring that servers do not experience an abrupt power failure from the loss of both main power and from the loss of battery backup power provided by the UPS devices.

4. We recommend the District transition its financial software to new hardware that uses a more modern operating system that can be supported through a vendor maintenance agreement.

5. We recommend that the District ensure that all of its UPS devices are operating optimally so that adequate battery backup power is available to support the servers when there is a main power failure.

6. We recommend that hardware and wiring located in the technology wiring closets be secured in locked cabinets to protect them from being dislodged or otherwise damaged.

AUDIT SCOPE, PROCEDURES AND FINDINGS *(Continued):*

Logical Controls / Data Access

- Review the District's Policies and Procedures related to data security.
- Evaluate the District's password parameters for adequacy.
- Determine whether procedures are adequate for establishing network accounts for new employees.
- Determine whether user privileges are adequately controlled through Active Directory or other means.
- Determine whether procedures are adequate to revoke or disable user accounts for terminated employees.
- Determine whether firewall reporting is monitored and reviewed by appropriate Technology staff.
- Determine whether anti-virus software is in place and is routinely updated with the latest definitions to provide adequate protections against viruses and malicious software.
- Determine whether USB drives are active on workstations, and whether there are restrictions from running executable files from flash drives.
- Determine whether employees are required to comply to terms outlined in acceptable use agreements.
- Determine whether controls are adequate for assigning user privileges in key systems, such as the financial accounting system.
- Perform vulnerability assessment procedures on points of entry into the District's network.

FINDINGS:

The controls over Data Access are operating effectively with the following exceptions noted:

1. The District's firewall, a CISCO ASA product, appears to be configured to provide adequate protections against inappropriate activities or malicious attempts related to incoming traffic to the District's network. However, the firewall does not appear to have been configured for egress filtering. Egress filtering would provide better controls on the outbound firewall traffic. No monitoring, reporting, or real time event notifications are in place.

AUDIT SCOPE, PROCEDURES AND FINDINGS *(Continued):*

Logical Controls / Data Access (*Continued*)

2. The District does not currently utilize software utilities that can assist in effectively monitoring firewall reporting. Firewall reporting can provide Technology staff and management with crucial information related to its performance and effectiveness in safeguarding the District's network from intrusions, vulnerabilities, or other inappropriate activities and network traffic. However, this reporting is often voluminous and difficult to manage. Software utilities are commonly used to assist in this process.

3. The District has not currently restrained the amount of bandwidth available to the wireless network. The District has established a wireless network that is available to students and guests. The wireless network is separate from the District's primary network that supports its main operating systems. However, the bandwidth that the wireless network utilizes is drawn from the District's total capacity of available bandwidth. That is, bandwidth used by the wireless network diminishes the amount remaining to be utilized by the primary network. Ultimately, the performance of the primary network can be negatively effected if sufficient bandwidth is not available to support the District's main operating systems. Software appliances are available and commonly used to apportion and manage capacity among various networks.

4. We noted that the District's anti-virus software appears to be receiving updates of the latest virus definitions regularly. However, the software is not currently configured to provide alerts to Technology staff about the results of recent scans and the status of workstations that may be at risk or out of compliance. Consequently, the correction action required to address vulnerable workstations may not be performed in a timely manner. We noted that there were 37 workstations that were not fully protected at the time of our review.

5. Microsoft routinely makes available updates and security patches for its operating systems. Organizations typically evaluate these updates to determine they will not cause operational complications to the network. Once the updates are approved they would automatically be pushed out and installed to the servers and computers. We noted that these updates have not been reviewed and approved by the District in a timely fashion in order to be deployed to servers and workstations. The District's virtualized servers were last updated in May 2014. We also noted that numerous Windows security updates deemed critical have not been deployed.

AUDIT SCOPE, PROCEDURES AND FINDINGS *(Continued):*

Logical Controls / Data Access (*Continued*)

6. Technology staff typically require credentials that have elevated privileges in order to perform their responsibilities for managing the network and workstations. However, these administrator rights are not necessary for all aspects of their job duties. A common method to safeguard the network and minimize the risk that administrator privileges could be potentially compromised is to establish two accounts for each Technology staff. One account would be a basic user account with rights similar to what most staff have. The second account, with elevated privileges, should only be used when the specific tasks being performed require administrator rights. We noted that Technology staff currently only have one account, with full administrator rights, which is used at all times. This increases the potential risk to the network in the event these credentials are compromised.

7. Our review identified a number of accounts with administrator rights that remain active but are not currently used by staff. They include:

    - An account for an EduTek engineer who left the District in 2014. The account password was never changed and the account remains active.
    - An account labeled "Network Administrator" is a generic account that remains active. It is not clear exactly which individuals had/has knowledge of the password and could access this account.
    - An account labeled "Administrator Hosting.com" is a generic account that remains active. It is not clear exactly which individuals had/has knowledge of the password and could access this account.

8. During, our review of employees who have left the District during the current school year, we identified the following instance in which an employee's access to the District's information system was not disabled in a timely fashion. Specifically, we noted:

    - A therapist retired in February 2015, but her account was not disabled until May 4, 2015, the day of our on-site visit.

AUDIT SCOPE, PROCEDURES AND FINDINGS *(Continued):*

Logical Controls / Data Access (*Continued*)

RECOMMENDATIONS:

1. We recommend the District strengthen its Internet security by installing a firewall that provides a higher level of protection via traffic inspection, anti-malware inspection at the gateway, advanced persistent threat monitoring, and logging/alerts. Examples of potential product vendors are Palo Alto Networks, Watchguard Security, and Cisco.

2. We recommend the District review the firewall rules and implement a stronger access control policy. The ingress and egress traffic filters should be reviewed and rules tightened to allow essential traffic only from the devices requiring access. Filtering the outbound traffic is as important as the inbound traffic.

3. We suggest the District consider restricting the amount of bandwidth that is made available to the wireless network in order to ensure that the remaining bandwidth available to the primary network is adequate for optimal performance. If the District feels that the primary network is operating adequately at this time, we recommend the District monitor the bandwidth used by the wireless network going forward in order to determine if/when it may become necessary to implement these restrictions in the future. An example of a product that provides visibility and control with an educational focus is Exinda Networks.

4. We recommend that the anti-virus software be configured to provide alerts to Technology staff that will communicate the results of scans and identify servers and/or workstations that may be vulnerable. Corrective action should be taken timely to address hardware that is not fully protected.

5. We recommend that Technology develop a plan to review and deploy Windows updates and security patches in a timely manner. The District should identify which staff will be responsible for managing this process. Completion of these tasks should be documented through the use of a checklist or log to be monitored by management. The Windows Update Server that is currently in use has reporting and logging capabilities which could be utilized.

6. We suggest the District consider implementing a process that requires Technology staff to utilize dual accounts. Their primary account should be a basic account with limited privileges, similar to other District staff. The account with administrator privileges should only be used in a limited fashion when necessitated by the specific task being performed. This practice can help to limit the risk to technology resources in the event that credentials become compromised.

AUDIT SCOPE, PROCEDURES AND FINDINGS *(Continued):*

Logical Controls / Data Access (*Continued*)

7. We recommend the District take corrective action to disable/delete all user accounts with administrator privileges that are not assigned to a specific individual and currently in use. Accounts with administrator rights are powerful accounts that should be limited both in the number of accounts created and in their use. An automated system for the logging of account information including logon, logoff and account modification events is also recommended.

8. It is important for access to information systems to be disabled immediately upon an employee's separation from the District. Although we acknowledge that Technology is likely to be aware of many employees that are leaving the District due to its relatively small size, we recommend that Technology work with Human Resources to develop a more formal notification process that will notify Technology of all terminations on the day (or effective date) they occur. Access to the network should be immediately disabled for all terminated employees. Requests to create and activate user accounts for new employees should also be formally communicated to Technology by a Human Resources employee that has been delegated with the authority to do so. The notification should provide specific permissions that are being requested for the new employee, rather than allowing Technology to make that determination. This notification could come in the form of an email. However, we also suggest the District consider implementing the use of a Personnel Action Form or a Technology Security form specifically designed for this purpose which could accommodate the internal control requirements for both new and terminated employees.

COMMENT:

Based on the limited vulnerability assessment procedures performed, the external firewall points of access appear to be filtered to allow access from only approved vendor networks.

To perform more detailed assessment procedures, the District's firewall would have to allow unfiltered access to our scanning server. This could be accomplished by the District configuring their firewall to grant access to our server. Additional assessment procedures could include a more comprehensive scan to evaluate network software issues behind the District's firewall, such as use of encryption, status of security patches, and so on.

AUDIT SCOPE, PROCEDURES AND FINDINGS *(Continued):*

Data Backup and Disaster Recovery Plan

- Review the District's formal Disaster Recovery Plan.
- Inquire about the process for testing the Recovery Plan and evaluate documentation related to recent tests performed.
- Review the process for backing up the District's critical data and information systems..
- Examine the District's backup documentation to determine whether the types of backups (incremental, full, etc.) are adequate and that backups are current.

FINDINGS:

The controls over the Data Backup and Disaster Recovery Plan aspect of our testing are operating effectively with the following exceptions noted:

1. The District does not appear to have documentation related to any formal testing that has been performed to determine whether data backup and disaster recovery procedures are adequate and functioning properly. Consequently, we were unable to determine whether current procedures can be relied upon to restore critical data in the event of a hardware failure or other crisis.

2. The District currently contracts with a third party vendor (E-Vault) to perform backups of its financial software system and the home directory and files of key staff and management. Our review of the E-Vault backup logs identified that while the backups are being performed regularly, the current configuration of these backup procedures appears inadequate. All backups performed by E-Vault are incremental backups. A full backup establishes a point in time that can be used to establish a recovery point. However, the value of incremental backups is limited without a full backup because no baseline has been established. It should be noted that the District's critical information is also backed up by the BOCES Regional Information Center (RIC). Since the E-Vault backup procedures have been established as a precaution for purposes of redundancy, the risk posed by the current configuration is minimized.

3. The District's Disaster Recovery Plan is currently published and made available to the general public on the District's website. The plan includes specific information related to the District's hardware and infrastructure. The plan also includes the backup schedules and retention periods for data. Publicizing these specifics provides no value or benefit to the District, and could be utilized by parties with malicious intent to gain access to the network and/or cause harm to the District's infrastructure.

AUDIT SCOPE, PROCEDURES AND FINDINGS *(Continued):*

Data Backup and Disaster Recovery Plan

RECOMMENDATIONS:

1. We recommend that Technology implement a process to document the specific tests of disaster recovery and backup procedures performed and the associated results. The recovery and return to operational status times should fall within the requirements of the District. This documentation should be retained and available for future reference.

2. We recommend that Technology modify its configurations of the backups performed by E-Vault. These backups should include periodic full backups in order to establish a baseline which can be used as a point in time to which to recover. The local backups performed in each building should not be hosted on a device in the same physical location. Utilizing backup storage in the far end campus location would minimize loss of primary and backup data stored in the same room or building.

3. We suggest that the District remove its Disaster Recover Plan from their website. Specific information related to hardware and infrastructure does not need to be made available to the general public.

CLOSING REMARKS:

We would like to thank Colin Byrne and his staff for their assistance and cooperation in regards to our audit of the Information Technology Department of the District.