South Orangetown Central School District
Internal Audit Report on
Information Technology

TABLE OF CONTENTS

R.S. ABRAMS & CO., LLP
Accountants & Consultants for Over 75 years

Robert S. Abrams *(1926–2014)*

Marianne E. Van Duyne, CPA
Alexandria M. Battaglia, CPA
Brendan Nelson, CPA

Board of Education
South Orangetown Central School District
160 Van Wyck Road
Blauvelt, NY 10913

We have been engaged by the Board of Education (the "Board") of the South Orangetown Central School District (the "District") to provide internal audit services with respect to the District's internal controls related to information technology for the period July 1, 2021 through February 28, 2022.

The objectives of the engagement were to evaluate and report on the District's internal controls pertaining to information technology and to test for compliance with laws, regulations, and the District's Board policies and procedures.

In connection with the following procedures, we have provided findings and recommendations for the internal controls related to information technology. Our procedures were as follows:

- Reviewed the District's policies, procedures, and practices with regards to the internal controls related to information technology;
- Interviewed key District employees involved in the information technology processes;
- Reviewed the District's information technology services contracts, for which a third party collects personally identifiable information, and Parents' Bill of Rights to ensure compliance with Education Law §2-d;
- Reviewed the District's annual notifications required under the Family Educational Rights and Privacy Act for the required elements;
- Performed a physical observation of the District's Main Distribution Facility (MDF) located at the High School and MDF located at the Middle School to verify the server rooms were properly secured and that the servers were reasonably protected from fire and floods;
- Reviewed user accounts for the District's network to identify multiple active user accounts, generic user accounts, and ensure individual accounts are associated with current, active District employees;
- Reviewed the access controls surrounding the District's network, accounting information system, student information system, and special education student management system;
- Reviewed the user permissions within the accounting information system to identify possible permissions granted to employees that may not be consistent with their job responsibilities;
- Reviewed the District's *Disaster Recovery Plan* to determine that the Plan identified critical information technology infrastructure and equipment, established the most suitable recovery

strategy for each application utilized by the District, and identified those individuals responsible for overseeing the disaster recovery process.

The results of our procedures are presented on the following pages.

Our procedures were not designed to express an opinion on the internal controls related to information technology, and we do not express such an opinion. As you know, because of inherent limitations of any internal control, errors or fraud may occur and not be prevented or detected by internal controls. Also, projections of any evaluation of the accounting system and controls to future periods are subject to the risk that procedures may become inadequate because of changed conditions.

We would like to acknowledge the courtesy and assistance extended to us by personnel of the District. We are available to discuss this report with the Board or others within the District at your convenience.

This report is intended solely for the information and use of the Board, the Audit Committee and the management of the District and is not intended to be and should not be used by anyone other than those specified parties.

Very truly yours,

R.S. Abrams & Co., LLP

R.S. Abrams & Co., LLP
March 30, 2022

GOVERNANCE

Policies and Procedures

The District is responsible for maintaining compliance with Education Law §2-d and the Family Educational Rights and Privacy Act (FERPA) which provide clear protections for student data. The District has adopted a comprehensive set of formal Board policies relating to information technology as required by the New York State School Boards Association. The *District Technology Plan* discusses the District's plans for instructional technology, hardware, software, implementation, and infrastructure inventory. The plan specifically covers District policies related to data backup, hardware and equipment, email, network accounts, network security, wireless access, and software.

Insurance

Cyber and privacy liability exposure is a growing risk for governmental entities. Data breach trends include hacking, lost or stolen laptops, backup tape loss, human error, and vendor or business partner breaches. Data breach incidents may be accidental, intentional or both. The costs related to governmental cyber and privacy breaches can be extreme. Some of these costs may include crisis service costs, legal costs, and replacement costs. As a result, cybersecurity insurance is becoming increasingly popular among governmental entities. cybersecurity insurance could reduce the number of cyber-attacks by promoting the adoption of preventative measures for increased protection and encouraging best practices. The District currently has a cybersecurity insurance policy with New York Schools Insurance Reciprocal (NYSIR).

Information Technology Services Contracts

The District contracts with the Board of Educational Services ("BOCES") for some information technology services. As part of their agreement with the District, BOCES provides services including but not limited to curricular support software and training as well as support and maintenance of the special education student management system, *IEP Direct*. The District utilizes *PowerSchool* for student data management. This application allows the District to track attendance, behavior, grades, and scheduling by student. The system assists the District in preparing required reports submitted to the New York State Education Department.

Disaster Recovery Plan

The District is in the process of finalizing a *Disaster Recovery Plan* that includes procedures related to preparing for recovery or continuation of technology infrastructure critical to the District after a disaster. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications such as networking, and other information technology infrastructure. While districts would like to ensure zero data loss and zero time loss in the event of a disaster, the cost associated with that level of protection may make the desired high availability solutions impractical. The primary goal of the District's Plan is to restore operations quickly and with the most current data available. Under the Plan, additional objectives include, but are not limited to the following:

- Developing an orderly course of action for restoring critical computing capability;
- Making the decision to recover at a cold site or repair the affected site;
- Developing an organizational structure to carry out the plan; and
- Identifying the equipment, floor plan, procedures, and other items necessary for recovery

NETWORK AND NETWORK SECURITY

Firewalls and Intrusion Detection Systems

A firewall is used to implement access control between two networks. It allows the District's network users to access outside information while preventing those outside the District from accessing the District's systems. The District utilizes an antivirus program created by CSINY, a cybersecurity company headquartered in Poughkeepsie, New York. This District also contracts with BOCES to maintain the District's firewall.

An intrusion detection system ("IDS") is a device or software application that monitors a network or systems for malicious activity or policy violations. The system blocks or drops traffic in response to a suspicious event identified by the IDS. The IDS will block traffic if it is detected as malicious based on protocols set to handle malware, blacklist, SQL injections and exploit-kit. The IDS sends alerts of suspicious activity to the Director of Technology and the information technology department. In addition, IDS logs are reviewed by BOCES and the information technology department.

Physical Security

The District's Network Operations Center (the "NOC"), is located at the High School. The NOC and other *Main Distribution Frames* ("the MDFs"), located at the other District locations, are the primary network locations that house approximately four physical servers and two virtual servers. Additionally, there are eighteen *Intermediate Distribution Frames* (the "IDFs") throughout the District. All server rooms are physically secured and have uninterrupted power supply ("UPS") units in place to protect the District's equipment from an unexpected power disruption that could cause business disruption or data loss. MDFs are also temperature controlled.

Backup Controls

The District's backup controls include utilizing the Lower Hudson Regional Information Center's remote backup service which is stored on a combination of disk and tape at their 450 Mamaroneck Avenue, Harrison, New York facility, and an auxiliary copy is maintained on disk at the off-site facility in West Nyack, New York. For any servers hosted at the BOCES data center, backups to tape are also sent to Iron Mountain for off-site storage and protection. Systems are backed up with a centralized backup solution using *Simapana Commvault*. All servers in the BOCES data center are backed up using this solution. All backups are encrypted in transit and at rest. Encryption in transit is when the encrypted data is active, moving between devices and networks such as the internet, within a company, or being uploaded in the cloud. Encryption at rest is defined as not being actively used, such as moving between devices or networks. This information is stored in one location on hard drives, laptops, flash drives, or cloud storage. Data is encrypted at rest through hardware-based software and devices. Backups are periodically restored to ensure data is available and the backup process is running correctly.

Network and Email Access

The District utilizes *Microsoft Exchange 365* for the District's email service and the District uses *Active Directory* synchronization for the authentication of network users. The Director of Technology and the information technology team are responsible for system administration. A *New Employee Information Form* is completed for all employees who need new access to the District's network and other applications. For new employees, the employee information is completed by the human resources department and BOCES completes the technology related section of the form which authorizes all user permissions the new employee requires. When new teachers are hired, they are required to complete information technology training which includes a review of the District's best practices for security.

Network Security

The District is currently engaged in a project to begin utilizing Multifactor Authentication ("MFA"). MFA is a security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction. The District will be contracting with Microsoft for the MFA in conjunction with USB Security keys.

Remote Access

The District no longer provides end-users with access to network resources via Virtual Private Network. Access to the Remote Desktop *VMWare* is provided when the users network account is created. Access and permissions are based upon the users' Active Directory rights and permissions.

Passwords

Access to computerized files and transactions should be restricted to authorized individuals only. This can be accomplished through the use of passwords and software that restricts user access to help ensure that only authorized individuals utilize the computer system. *Active Directory* network user passwords consist of a minimum of eight characters and must meet complexity requirements (at least one of each character type, such as uppercase, lowercase, numeric, and symbolic). Users are required to change their passwords every 90 days. The District's password lockout policy is the same between the administrative and instructional networks. Both the administrative and instructional networks are set to lockout users after five invalid login attempts.

STUDENT DATA SECURITY

Student Information System Access

PowerSchool Student Information System ("*PowerSchool*") is the student data management application currently utilized by the District, which allows the District to track attendance, behavior, and grades by student. The system also provides a course catalog, graduation planning, a grade book, and assists the District in preparing required reports submitted to the New York State Education Department. The entire system is web-based, which allows teachers, instructional administrators, instructional clerical staff, and parents to access student information. Further restrictions are applied to the individual's user privileges to ensure that only authorized users have access to sensitive information.

IEP Direct Access

IEP Direct is the special education student management application currently utilized by the District. *IEP Direct* is a web-based application that is utilized in conjunction with *PowerSchool*, to track student IEPs, evaluations, meetings, and assists with the preparation of New York State required reports. Additionally, *IEP Direct* enables the preparation of STAC forms, facilitating the recovery of Medicaid funds. The system has an optional Medicaid Direct add-on that automates the Medicaid tracking and billing process for maximizing revenue recovery by improving data accuracy and accelerating collections. *IEP Direct* also facilitates District compliance with applicable privacy laws and regulations.

Data Breach – Sensitive Personally Identifiable Information ("PII")

A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or utilized by an unauthorized individual. The District PII is stored in *Infinite Campus, IEP Direct,* and *nVision*. The District prohibits third party access to the PII data with the exception of the application vendor. District employees are instructed to use *Zix Corp.* to encrypt and secure PII through email. The District has adopted Board policy No. 8635 and related regulation 8635-R, *Information Security Breach and Notification* which identifies the need to secure "private information" and procedures

to be followed in the event of a breach. The District is not aware of any incidents of data breach of their PII data.

ACCOUNTING INFORMATION SYSTEM

The District utilizes *nVision* as its accounting information system (AIS). This application was installed and managed by BOCES who handles all required application updates, database management, data back up and if necessary, system restorations. The District performs a variety of functions within the accounting information system including but not limited to budget development, accounting, requisitions, receivables, and payroll. Access to *nVision* must be initiated by the District Treasurer or the Director of Technology via an email to BOCES. A member of the BOCES financial team will then either create a new account or make changes to an existing account based on the responsibilities of the employee requiring access.

Permissions and Passwords

The District has procedures in place to periodically verify the system of controls are working as intended, are still needed, and are cost effective, including a review of the controls over access to information systems. Access to computerized files and transactions should be restricted to authorized individuals only. This can be accomplished with the use of passwords and software that can restrict a user's access and can help ensure that only authorized individuals utilize the computer system. Network passwords consist of at least six characters, must not contain the user's account name that exceed two characters, and must contain characters from three of the four following categories: uppercase characters, lowercase letters, base 8 digits and a non-alphabetic character. Additionally, network passwords need to be changed every 90 days. The District has a password lockout policy whereby after ten failed attempts, the employee will be prevented from signing into the network. It should also be noted, *nVision*, the Accounting Information System, has maximum login attempts of three times. Passwords for *nVision* are required to be changed every 30 days.

FINDINGS AND RECOMMENDATIONS

Based on our interviews, observations, and detailed testing, we have provided our findings and recommendations below to further strengthen the District's internal controls as they pertain to information technology outlined above.

It should be noted that these recommendations are provided to the District to assist management in improving the District's internal controls and procedures relating to information technology. It is important to note that our findings and recommendations are directed toward the improvement of the system of internal controls and should not be considered a criticism of, or reflection on, any employee of the District.

***

Policies and Procedures

Procedure Performed: We reviewed the District's policies and procedures with regard to the internal controls related to information technology.

Finding: No exceptions were noted as a result of applying these procedures.

***

Information Technology Services Contracts/Parents' Bill of Rights

Procedures Performed: We reviewed the District's Parents' Bill of Rights to ensure compliance with *Education Law §2-d* and the information technology services contracts who collect personally identifiable information.

Finding: No exceptions were noted as a result of applying these procedures.

***

Required Annual Notifications

Procedures Performed: We reviewed the District's annual notifications required under the *Family Educational Rights and Privacy Act* for the required elements.

Finding: No exceptions were noted as a result of applying these procedures.

***

Server Rooms

Procedures Performed: We physically inspected the District's IDFs located at the High School and Middle School to verify the server rooms are properly secured, monitored, and that the servers are reasonably protected from fire and floods. We also inquired of the other network facilities located throughout the District.

Finding: No exceptions were noted as a result of applying these procedures.

***

Permissions/Access Controls

Procedure Performed: We reviewed the access controls surrounding the District's network, accounting information system, student information system, and special education student management system.

Finding: No exceptions were noted as a result of applying these procedures.

***

Procedure Performed: We reviewed the user permissions within the student information system and special education student management system to identify possible permissions granted to employees that may not be consistent with their job responsibilities.

Finding: No exceptions were noted as a result of applying these procedures.

***

Procedure Performed: We reviewed the user permissions within *nVision* to identify possible permissions granted to employees that may not be consistent with their job responsibilities.

Finding: No exceptions were noted as a result of applying these procedures.

***

Disaster Recovery Plan

Procedure Performed: We reviewed the District's Disaster Recovery Plan (the "Plan") to determine that the Plan identifies critical information technology infrastructure and equipment, establishes the most suitable recovery strategy for each application utilized by the District, and identifies those individuals responsible for overseeing the disaster recovery process.

Finding: No exceptions were noted as a result of applying these procedures.

CORRECTIVE ACTION PLAN

The District is required to prepare a corrective action plan in response to any findings contained in the internal audit reports. As per Commissioner's Regulations §170.12, a corrective action plan, which has been approved by the Board, should be submitted to the State Education Department within 90 days of the receipt of a final internal audit report.

The approved corrective action plan and a copy of the respective internal audit report should be submitted using the NYSED Business Portal.