OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Avon Central School District

Information Technology

Report of Examination

Period Covered:

July 1, 2014 – February 26, 2016

2016M-123

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

July 2016

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help local school district officials manage their districts efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as districts' compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving district operations and Board of Education governance. Audits also can identify strategies to reduce district costs and to strengthen controls intended to safeguard district assets.

Following is a report of our audit of the Avon Central School District, entitled Information Technology. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law.

This audit's results and recommendations are resources for district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

Introduction

Background

The Avon Central School District (District) is located in the Towns of Avon, Caledonia, Lima and York in Livingston County and the Town of Rush in Monroe County. The Board of Education (Board), composed of five elected members, governs the District. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The District uses network and Internet resources to support certain business operations, such as providing communication, maintaining student records, performing online banking transactions and maintaining financial records, including personal, private and sensitive information (PPSI). The Technology Coordinator is responsible for managing network security and data. District officials are responsible for creating and implementing information technology (IT) policies to help ensure that security is maintained over the network and data.

The District operates three schools with approximately 1,000 students and 190 employees. The District's budgeted general fund appropriations for the 2015-16 fiscal year totaled $19.2 million, which was funded primarily with State aid and real property taxes.

Objective

The objective of our audit was to assess the District's IT. Our audit addressed the following related question:

- Has the Board ensured that the District's IT assets and computerized data are safeguarded?

Scope and Methodology

We assessed the Board's oversight of IT assets and computerized data for the period July 1, 2014 through February 26, 2016. Our audit also evaluated the adequacy of certain IT controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to District officials.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix B of this report.

Comments of District Officials and Corrective Action

The results of our audit and recommendations have been discussed with District officials, and their comments, which appear in Appendix A, have been considered in preparing this report. District officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education, a written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, with a copy forwarded to the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The Board should make the CAP available for public review in the District Clerk's office.

Information Technology

IT assets and computerized data are valuable resources that District officials rely on for making financial decisions, processing transactions, keeping records and reporting to State and federal agencies. The potential consequences of an IT system failure range from inconvenient to severe. Accordingly, District officials are responsible for establishing, designing and implementing a comprehensive system of internal controls over the District's IT system.

The Board is responsible for adopting formal policies focused on protecting data and hardware from loss or misuse due to errors, malicious intent or accidents (e.g., disasters). Therefore, it is essential that the Board establish policies that include password management; wireless technology; remote access; use of mobile devices; data backups; sanitation and disposal of electronic media; breach notification; user accounts; access rights; and the protection of personal, private and sensitive information (PPSI). The Board should periodically review and update these policies as necessary to reflect changes in technology or the District's IT environment. In addition, financial software access should be limited to just those applications, resources and data that are necessary for a user's day-to-day duties and responsibilities. A disaster recovery plan should be developed to prevent the loss of computerized data and to help District personnel resume operations in the event of a disaster.

The Board did not adopt policies for password management, protection of PPSI, wireless technology, remote access, mobile devices, sanitation and disposal of electronic media, user accounts, access rights, data backups and breach notification. In addition, the Business Manager had administrative rights to the financial software that provided her with the ability to add or update user access rights and add, delete, change or modify data. The Business Manager was unaware that she had administrative rights, and upon learning this, BOCES staff removed her administrative rights. The Board also did not adopt a disaster recovery plan. As a result, there is an increased risk that the District's IT data and components will be lost or misused and that the District will not be able to resume critical operations in the event of a system failure.

Security Policies and Procedures

IT security policies describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. Therefore, it is essential for the Board to establish IT security policies for all IT assets and information.

The Board should periodically review these policies, update them as needed and stipulate who is responsible for monitoring IT policies.

Although the Board adopted policies for acceptable use and online banking, it has not adopted other IT security policies addressing password management, protection of PPSI,[1] wireless technology, remote access, mobile computing and storage devices, sanitation and disposal of electronic media, user accounts, access rights and data backups. The technology coordinator documented limited written procedures for backing up data that are documented in the District's technology plan. However, the Board did not adopt this plan. The District's previous internal audit from 2009 also recommended that the Board adopt certain IT policies, including a policy for password management. However, the Board did not adopt these policies. The technology coordinator did not develop any written procedures for these areas until we asked about it during our fieldwork.

While IT policies do not guarantee the safety of the District's IT assets or electronic information, the lack of policies significantly increases the risk that data from hardware and software systems may be lost or damaged by inappropriate access and use. Without formal policies that explicitly convey the appropriate use of the District's computer equipment and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities.

Breach Notification

An individual's private and financial information, along with confidential business information, could be severely affected if the District's computer security is breached or data is improperly disclosed. New York State Technology Law requires local governments to establish an information breach notification policy. While school districts are not subject to this law, it is still in the District's best interest to adopt and implement such a policy. The policy should detail how officials would notify residents whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure should be made in the most expedient time possible without unreasonable delay, consistent with the legitimate needs of law enforcement or any measure necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The Board has not adopted a breach notification policy. By failing to adopt an information breach notification policy, in the event that private information is compromised, District officials and employees may not understand or be prepared to fulfill their obligation to notify affected individuals.

[1] Such as practices to safeguard when collecting, storing or transmitting confidential information

Financial Software Access Rights

District officials are responsible for restricting users' access to just those applications, resources and data that are necessary for their day-to-day duties and responsibilities to provide reasonable assurance that computer resources are protected from unauthorized use or modifications. User accounts enable the network and applications to recognize specific users, grant them appropriately authorized access rights and provide user accountability for transactions. Generally, an administrator is designated as the person who has oversight responsibility and control of an application. Users with administrative access rights can create, delete and modify user accounts and access rights; make adjustments to application security and settings; and record or adjust entries. Therefore, administrative access rights must be limited and assigned to someone independent of any Business Office function.

Each user of the District's financial software is assigned a unique user account to enable access rights to be assigned based on the resources and information needed to perform their job duties and enhance accountability. We reviewed the access rights granted to users of the financial software and identified two individuals who had more rights than necessary to perform their duties. Although Wayne-Finger Lakes Board of Cooperative Educational Services (BOCES) Edutech staff members are designated as the administrators of the software, the Business Manager also had administrative rights to the financial software, which provided her with the ability to add or update user access rights and add, delete, change or modify data.

One of the BOCES staff members with administrative rights also had full access rights to the entire software application, instead of limited access to perform only the administrative tasks as intended. These users were not authorized to have these access rights, and until we inquired about the access rights, District officials and BOCES staff were unaware that these individuals had this access. After we brought this to their attention, these inappropriate access rights were immediately removed by BOCES.

This type of access could allow users to make unauthorized changes to the accounting records, financial software security settings and user access rights. Further, users with unnecessary access rights could lead to the loss of important financial data, interruptions to District operations or the inappropriate use of District assets. Although a process was not in place to review these rights on a periodic basis, we commend the District and BOCES for taking swift corrective action once this weakness was brought to their attention.

Disaster Recovery

A disaster recovery plan provides a framework for reconstructing vital operations to ensure the resumption of time-sensitive operations

and services in the event of a disaster. Such disasters may include any sudden, catastrophic event (e.g., fire, computer virus, power outage or a deliberate or inadvertent employee action) that compromises the availability or integrity of the IT system and data. The plan should detail the precautions to minimize the effects of a disaster and enable the District to maintain or quickly resume critical functions. The plan should include a significant focus on disaster prevention and should be distributed to all responsible parties, periodically tested and updated as needed.

The Board has not adopted a comprehensive disaster recovery plan to address potential disasters. The District has an outdated and inadequate technology plan that includes a section for disaster recovery. However, this plan was not adopted by the Board, is not comprehensive and has not been updated since 2009. For example, the plan lists the emergency facility for District operations as the District Office[2] and does not provide an alternate work location in the event of a disaster that destroys this location.

The technology plan is on the District's website and administrators involved in its development back in 2009 were provided with copies. However, District officials, including those identified in the plan as critical personnel, were either not aware of the plan or not familiar with the details contained within the plan. Consequently, in the event of a disaster, the lack of familiarity of the plan by District officials and personnel greatly hinders the likelihood that the plan would be used and implemented. Further, an inadequate and outdated disaster recovery plan increases the likelihood that the District could lose important data and suffer a serious interruption in time-sensitive operations, such as processing payroll or checks to vendors.

Recommendations

The Board should:

1. Adopt policies and procedures for password management, protection of PPSI, wireless technology, remote access, mobile devices, sanitation and disposal of electronic media, user accounts, access rights, data backups and breach notification.

2. Periodically review policies and procedures, update them as needed and stipulate who is responsible for monitoring all IT policies.

3. Develop a formal disaster recovery plan to maintain or restore critical operations as quickly as possible in the event of a

[2] The District Office is located in the same building as the middle school and high school.

disaster. This plan should be distributed to all responsible parties, periodically tested and updated as needed.

District officials should:

4. Institute a process to periodically review assigned access rights and ensure access rights are based on job duties.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

The District officials' response to this audit can be found on the following page.

Avon Central Schools

191 Clinton Street · Avon, New York 14414-1495
(585) 226-2455
www.avoncsd.org

Aaron R. Johnson, Ed.D., Superintendent
Kristen A. Murphy, Business Manager
Jason R. Shetler, High School Principal
Jennifer K. Miller, Middle School Principal
Robert T. Lupisella, Primary School Principal
Kelly L. White, Director of Pupil Services, Curriculum, and Instruction

Rodney George, Board of Education President
James Colt, Vice-President
Robert DeBruycker
David Peck
Jim Ryan

June 2, 2016

Mr. Edward V. Grant Jr.
Chief Examiner
The Powers Building
16 West Main Street Suite 522
Rochester, New York 14614-1608

Dear Mr. Grant:

This letter is to acknowledge the receipt of the DRAFT Report of Examination- Information Technology for the period of July 1, 2014 – February 26, 2016 issued by the NYS Office of the State Comptroller for the Avon Central School District. On behalf of our Board of Education and our school community, I would like to thank your team for their attentive care and professionalism throughout the recent audit process. Your examiners were respectful in their approach and considerate to our personnel as they balanced the needs of their daily work with those of an active school building. The result was a product that we find to be both fair and informative.

Here at Avon we strive to be reflective and open to feedback in all that we do. Our staff and students ground themselves in the work of Carl Dweck and the affirmation of a growth mindset. Feedback like that found in the DRAFT report is an opportunity for our organization to model this mindset for our constituents in an effort to fuel our continued improvement. In this digital age our reliance on technology for both operations and instruction is vital. Policies to govern this use provide guideposts to promote cybersecurity. Thank you for identifying areas within our information technology that are current gaps in these protective measures. Your feedback will help us to safeguard the vital financial and personal information of our District to the best of our ability.

Immediately after sitting down with your staff for our informal post-audit meeting, we began working to address the suggestions given. At a recent Board of Education meeting the first recommended policy was adopted and others are in the queue. Although we did have many appropriate "practices" in place, the point made about Board directed policy was a good reminder. These new information technology policies and an updated disaster recovery plan will leave Avon better informed and prepared should a threat present itself.

In close, we greatly appreciate the time taken by your examiners to ensure a comprehensive and meaningful report. We embrace this opportunity to make improvements to our practice and value the recommendations provided by your staff as resources to promote the effective management of our operations.

Sincerely,

Aaron R. Johnson, Ed.D
Superintendent of Schools

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

To achieve our audit objective and obtain valid audit evidence, we performed the following audit procedures:

- We interviewed District officials and employees to gain an understanding of the IT environment and internal controls in place.
- We reviewed the financial software user access report and compared the granted access rights to the users' job duties and determined the access rights needed for those duties.
- We reviewed the District's policies, technology plan and Board minutes for existing IT policies and procedures.
- We observed computer screen shots to verify certain supporting statements made by employees.
- We reviewed a 2009 audit report from the District's internal auditor that reviewed the District's IT operations.

We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX D

OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE
Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington Counties

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates Counties

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence Counties

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313