OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Livonia Central School District

Software Management

Report of Examination

Period Covered:

July 1, 2014 – April 1, 2016

2016M-293

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

December 2016

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help district officials manage their district resources 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 Livonia Central School District, entitled Software Management. 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 Livonia Central School District (District) is located in the Towns of Avon, Conesus, Geneseo, Groveland, Lima, Livonia and Springwater in Livingston County and the Town of Canadice in Ontario County. The District is governed by the Board of Education (Board), which comprises seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer of the District and is responsible, along with other administrative staff, for the day-to-day management of the District under the Board's direction.

The Director of Information Technology (Director) works closely with the Superintendent to meet the directives of the Board. The Director and her staff are responsible for the day-to-day management of the District's information technology (IT) infrastructure.

The District operates three school buildings with approximately 1,600 students and 350 employees. The District's budgeted appropriations for the 2016-17 fiscal year are approximately $33 million, which are funded primarily with State aid, real property taxes and grants.

Objective

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

- Have the Board and District officials effectively managed the District's software to ensure that the District's IT assets and computerized data are safeguarded?

Scope and Methodology

We examined the District's use of its IT infrastructure for the period July 1, 2014 through April 1, 2016. Our audit disclosed areas in need of improvement concerning IT controls. Because of the sensitivity of some of this information, certain vulnerabilities are not discussed in this report but have been communicated confidentially to District officials so they could take corrective action.

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 have taken, or plan to take, corrective action.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of General Municipal Law and Section 170.12 of the Regulations of the Commissioner of Education, a written corrective action plan (CAP) that addresses the 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 should 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's Administration Office.

Software Management

The management of software and licenses is essential to safeguarding District assets and data. Therefore, District officials must have an understanding of the software the District owns, how it is used and how best to track user rights to ensure licensing compliance. The effective management of software also includes ensuring that only appropriate business or academic software is installed to reduce the risk of unwanted consequences and unnecessary costs that could result from unauthorized software. This can be done, in part, by regularly reviewing computers to identify installed software and taking action to remove any unauthorized software. Additionally, District officials must ensure that software, patches and virus protections are up-to-date to reduce vulnerabilities. Finally, IT administrators should develop a disaster recovery plan to prevent the loss of computerized data and to help District personnel resume operations in the event of a disaster, such as IT disruption due to malware or software malfunction.

The District should manage its software more effectively and efficiently. The Board's acceptable-use policies are inadequate because they do not detail practices for enforcement, such as monitoring computer use and reviewing installed software, or include specific penalties for noncompliance. IT staff does not maintain a comprehensive inventory of all software that the District owns and for which it purchased licenses. In addition, District officials and IT staff do not regularly monitor or review District computers to ensure that all software installed by the user is up-to-date, appropriate and legally obtained and that virus protection and patches are installed and up-to-date. As a result, 21 of the 40 computers in our test sample had improper software applications that included software for a personal cell phone, Internet television services, a coupon application and an Internet parental monitoring application. In addition, we found five instances of malware and significant personal use by 16 users. The installation of nonbusiness, noneducational or unlicensed software may be exposing District computers and networks to unnecessary risks, such as copyright infringement, hacking or other malicious events. Because the Director did not develop a disaster recovery plan, as required by Board policy, 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 or ransomware attack.

Software Inventory

Software management is of particular importance to larger entities, such as the District, that have many different users who perform a variety of functions. Typically, these organizations will have several software applications and multiple licenses for each. The

implementation of a complete and comprehensive software inventory list is crucial to safeguard IT assets from potential unauthorized and unlicensed software being installed on computers. As a best practice, the list should include all District-owned software installed on computers and the number of copies currently in use. Furthermore, the list should be used in conjunction with a comprehensive hardware inventory list that details computer locations and users, in conjunction with regular reviews of all computers owned by the District, to ensure that all software installed is properly approved and licensed. Finally, software additions or changes should be made by IT administration, when practical, to ensure that the software works well with the network, is safe to use and is for business use.

The purpose of a software license is to grant an end user permission to use one or more copies of a software program in accordance with copyright law. When a software package is sold, it is generally accompanied by a license from the manufacturer that authorizes the purchaser to use a certain number of copies of the software. Organizations must obtain licenses commensurate with the number of copies in use. The penalties for software licensing violations can be severe, exposing the District to legal liability, additional attorneys' fees and the expense of mandated IT audits.

District officials and IT staff did not maintain a comprehensive software inventory of District-owned software programs and their applicable licenses. Although District officials can generate a report of hardware and software purchased, they do not do so, and the report generated for our review did not summarize or clearly define the total number of licenses for each software application.[1] District officials also did not maintain and could not generate a report that listed all installed applications and the specific computers on which these applications are installed. The Director told us there were no formal procedures for the regular review of computers to determine software installed; instead, an informal review process was sometimes performed during the summer as staffing allowed.

Because District officials did not maintain a comprehensive software inventory list and IT staff do not perform regular, formal reviews of District computers, District employees and students were able to install inappropriate software on computers without detection,[2] which put the District's network at a high risk of intrusion and corruption. Our review of the 40 District computers in our sample found that 398 of the 442 (90 percent) installed software applications were not on the District's software inventory list.

[1] After our further inquiry, District officials researched recent software purchases and determined the number of licenses that were purchased.

[2] Refer to the Software Monitoring section for further information.

Software Monitoring

The District's acceptable computer use policies provide users with guidelines for IT asset use and security. Specifically, the District encourages users to support professional and personal development in the educational community and expects all users to use electronic communications in a responsible manner. The District requires users to adhere to the laws, policies and rules governing computers, including copyright laws and rights of software publishers and license agreements, and reserves the right to restrict or limit access or use based on violations of laws or agreements. Users are also prohibited from using IT resources to harass or harm individuals.

The District's adopted acceptable-use policies[3] lack specific guidance related to software installation and usage. The policies do not describe enforcement practices, such as monitoring computer use and reviewing installed software, or include penalties for noncompliance. Therefore, to determine if installed software was appropriate, we selected 40 of the 1,500 District computers[4] for review. We found the 442 software programs[5] installed on the computers were generally appropriate and up-to-date. However, 21 computers had 45 inappropriate software program installations that were not business- or academic-related, including five software applications that had the potential to contain malware,[6] a coupon application, photo and video editing software and an Internet parental control application.

Because over half of the reviewed computers contained inappropriate software, we performed additional testing and determined that 16 of the 40 (40 percent) users were using District computers on a more than incidental basis for personal use. For example, we identified six computers with excessive personal photos, ranging from 167 to over 4,200. Another user had 388 items in her recycle bin, mostly spreadsheet files related to her personal business.

Although the District's acceptable-use policies do not expressly prohibit computer use for nonbusiness or noneducational purposes, non-District-related programs may interfere with employees' work responsibilities and may expose the District's computers and networks to unnecessary risks, such as viruses, malware, hacking or other malicious events. Furthermore, District computers and software

---

[3] The Board has adopted the following policies regarding computers: Staff Use of Computerized Information Resources, Use of Email in the School District and Internet Safety/Internet Content Filtering.

[4] See Appendix B, Audit Methodology and Standards, for more information.

[5] A portion of which included components of larger software programs

[6] The National Institute of Standards and Technology defines malware (also known as malicious code and malicious software) as a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim's data, applications or operating system or otherwise annoying or disrupting the victim.

should not be used for private businesses and this should be clearly stated in the acceptable-use policy. Because regular reviews of District computers were not performed, inappropriate installations were not identified and removed in a timely manner. Further, without proper documentation, the District cannot ensure that its software programs are properly licensed and could incur fines or penalties for installing software applications that are not properly licensed or for using software purchased for educational purposes for a private business.

Disaster Recovery

The impact of an unplanned IT disruption, involving the corruption or loss of data or other computer resources caused by human error, malware or hardware failure could significantly curtail the District's operations. Proactively planning for such IT disruptions will prepare District personnel for the actions they must take in the event of an incident. A disaster recovery plan provides a framework for reconstructing vital operations to ensure the resumption of time-sensitive operations after a 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 adopted a policy[7] in January 2016 that requires the Superintendent or his or her designee to develop a comprehensive disaster recovery plan to address potential disasters as appropriate to the District's size. However, as of July 2016, the District did not have a disaster recovery plan in place. As a result, the District's IT assets and data remain at an increased risk of loss, misuse or damage, and District operations could be seriously disrupted. This is of particular importance given the current prevalence of ransomware attacks.

Recommendations

The Board should:

1. Update the acceptable-use policies to include specific guidance related to software downloads and installations as well as enforcement. Policies should be regularly reviewed, updated and distributed to users to obtain their written agreement of compliance with the policy terms.

District officials should work with IT staff to:

2. Maintain a complete, comprehensive software inventory of all software that the District owns and the total number of licenses for each specific type of software.

[7] Entitled Data Networks and Security Access, adopted January 11, 2016

3. Formalize procedures to perform reviews of software installed on District computers and compare results to the District's software inventory list.

4. Monitor users to ensure compliance with the acceptable-use policies and ensure all software installed on District computers serves an appropriate business or educational purpose.

5. Develop a formal disaster recovery plan to maintain or restore critical operations as quickly as possible in the event of a disaster. This plan should be distributed to all responsible parties, periodically tested and updated as needed.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

LIVONIA
Central School District

P.O. Box E
Livonia, NY 14487-0489
www.livoniacsd.org

Matthew Cole, *Superintendent of Schools*
mcole2@livoniacsd.org
(585) 346-4000, ext. 4000
Fax: (585) 346-6145

November 10, 2016

Office of the State Comptroller
The Powers Building
16 West Main Street – Suite 522
Rochester, NY 14614

Office of the Comptroller:

On behalf of the Board of Education, please accept our appreciations for the courteous, professional, and informative field staff involved in our audit. This letter is to acknowledge receipt of the draft Report of Examination – Software Management 2016M-293 for the period of July 1, 2014 to April 1, 2016 issued by the NYS Office of the State Comptroller for the Livonia Central School District. The BOE and district staff is pleased with the extensive work of the auditors from your office and that the audit resulted in *NO findings of operational improprieties, fraud, waste, abuse, or excess reserves*.

The audit conducted an assessment of our software management capabilities, policies, and practices. The results of the audit are fair and informative. As noted throughout the process the District postponed upgrades to our software management due to significant reductions in NYS school aid through the Gap Elimination Adjustment which withheld over $9,441,138 in state aid dating back to the SY2010-11 budget. Furthermore, the underfunding of the Foundation Aid formula reduced the District's state aid an additional $11,671,644 during that same time frame. As a result, the District continued to manage with outdated technology infrastructure using the [redacted] Platform with an end of life date of 2011 until being able to allocate funding to replace the network software management over this past summer.

The report contains five (5) recommendations that have been or will be enacted prior to the submission of the Corrective Action Plan in the coming weeks.

Again, the Livonia Central School District and Board of Education thanks the Office of the State Comptroller field staff involved for their meaningful report which reinforced the need to update our technology infrastructure and software management capabilities. We value the meaningful report and appreciate the vote of confidence on the fiscal stewardship of the District.

Sincerely,

Matthew Cole, Superintendent

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

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

- We interviewed District officials and employees to gain an understanding of the IT operations.

- We reviewed the District's relevant policies and procedures, including those related to IT, for adequacy and to gain an understanding of the District's operations.

- We obtained a list of all District employees, sorted it based on job title and grouped the employees into three tiers based on their ability to override the implemented controls of the District's IT system. Tier One consisted of administrators, supervisors, managers and all IT staff. Tier Two consisted of all other teachers and staff not included in Tier One. Tier Three consisted of students. Each tier was then given a weight based on the tier's ability to override existing IT system controls. Tier One was weighted at 62.5 percent, Tier Two at 25 percent and Tier Three at 12.5 percent for the purposes of selecting a random sample for testing. From the sorted list, we selected a sample of 40 users based on risk (determined based on level of access rights, information the user had access to and the increased potential of sensitive information stored on the user's computer) and total users in each sorted tier. Each employee was then assigned a unique number value and a random number generator was used to select a random sample of 40 users/computers. We used specialized audit software to obtain a list of all software installed on each machine. We reviewed the installations to determine if they served a legitimate business purpose. In addition, we searched each computer for specific file extensions to determine if the computer was being used on a more than incidental basis for personal use.

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