OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Village of East Hampton

Information Technology

Report of Examination

Period Covered:

August 1, 2013 – April 30, 2015

2015M-187

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

November 2015

Dear Village Officials:

A top priority of the Office of the State Comptroller is to help local government officials manage government resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of local governments statewide, as well as 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 operations and Board of Trustee governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard local government assets.

Following is a report of our audit of the Village of East Hampton, 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 local government 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 Village of East Hampton (Village) is located in the Town of East Hampton in Suffolk County and has a population of approximately 1,400 residents. General fund expenditures for the 2013-14 fiscal year were approximately $19.7 million, which were funded primarily through real property taxes, license and permit fees and State and federal aid.

The Village is governed by an elected Board of Trustees (Board), which is composed of the Mayor and four Trustees. The Village contracts with an information technology (IT) consultant who administers network performance, computer systems repair, systems setup and configuration programming and diagnostics. The Treasurer serves as the administrator of the Village's financial software.

Objective

The objective of our audit was to determine if computerized data and assets were properly safeguarded. Our audit addressed the following related question:

- Have Village officials implemented effective internal controls over computerized financial data to safeguard Village assets?

Scope and Methodology

We examined the Village's internal controls relating to computerized financial data from August 1, 2013 through April 30, 2015. Our audit also examined 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 Village 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 C of this report. Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

Comments of Village Officials and Corrective Action

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

includes our comment on an issue raised in the Village's response letter.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and forwarded to our office within 90 days, pursuant to Section 35 of General Municipal Law. 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. We encourage the Board to make this plan available for public review in the Clerk's office.

Information Technology

The Village's IT system is a valuable and essential part of the Village's operations, used for Internet access, email and maintaining data and financial records. The potential consequences of a system failure can range from inconvenient to severe. Even small disruptions in processing can require extensive time and effort to evaluate and repair. Accordingly, Village officials should establish internal controls over IT to ensure that Village assets are protected against waste, loss and misuse. Effective IT controls include policies and procedures to address user access, remote access, password security and management, data backups and the assignment of user and administrative access rights only to specific identified system users based on their specific job duties. The Board should also adopt a comprehensive disaster recovery plan to address potential disasters.

The Board has not adopted written computer-related policies to address user access, remote access, password security and management, or data backups. Additionally, Village officials improperly assigned administrative privileges, created generic user accounts and provided excessive access rights to the Village's financial and real property tax software. For example, there are six generic user accounts[1] on the Village's computer network, including two with administrative access. In addition, the Treasurer has administrative rights to the financial software giving her the ability to add new users, create and change user access rights and make or delete evidence of payments without restriction. Further, the Clerk has supervisor level access to the real property tax software, giving her the ability to add, modify and delete property tax information and add, modify and delete user accounts. Finally, the Board has not adopted a comprehensive disaster recovery plan. As a result of these control weaknesses, Village officials' ability to determine responsibility for system activities is limited, and the Village's IT system and its data are subject to an increased risk of corruption, loss or misuse.

Policies and Procedures

Computer policies and procedures should define appropriate user behavior and the tools and procedures to protect data and information systems. The Board is responsible for creating an appropriate internal control environment over IT security. It should provide oversight and leadership by establishing computer policies and procedures that take into account people, processes and technology, and communicate these policies and procedures throughout the organization. The Board should adopt comprehensive policies addressing key security areas,

[1] Not affiliated with specific users

such as acceptable computer use, internal user access, remote access, password security and management, data backups and appropriate email and Internet use. For example, the Board is responsible for adhering to the New York State Technology Law that requires villages to establish a breach notification policy to describe how they would notify residents whose personal, private and sensitive information was, or is reasonably believed to have been, acquired by a person without a valid authorization.

While the Board has adopted policies for breach notification, acceptable computer use and the appropriate use of email and the Internet, it has not adopted policies or implemented procedures to address internal user access, remote access, password security and management, or data backups. Although comprehensive computer-related policies do not guarantee the security of the Village's electronic information, the lack of such policies significantly increases the risk that hardware and software systems and the data they contain may be lost or damaged by inappropriate access and use.

Network User Accounts

Network access controls limit or detect inappropriate access to computer resources, thereby protecting them from unauthorized modification, loss and disclosure. User identifiers (IDs) and passwords are the simplest and most common forms of user authentication to prevent unauthorized use or modification. User IDs enable the system to recognize specific user accounts, grant the appropriately authorized access rights and provide user accountability for computer transactions. User IDs must be affiliated with specific users and not shared among multiple users so Village officials can determine responsibility for system activities. Users with administrative access can assign user rights, access control permissions, install and uninstall applications and make adjustments to security and system settings. Therefore, administrative access must be limited and affiliated with specific users.

We reviewed all 52 user access accounts on the network and found the Village has six generic user accounts, which are used by multiple users, two of which have administrative rights to the server. The use of generic user accounts, including some with administrative access, makes the system vulnerable and limits Village officials' ability to determine responsibility for system activities and increases the risk that sensitive or critical data may be lost or compromised.

User Access to Application Software

To protect computer resources from unauthorized use or modification and ensure proper segregation of duties, user access rights should be assigned to officials and employees based on their job responsibilities. Administrator rights allow users to create, delete and modify files, folders or settings, including the assignment of users' access rights.

Generally, an administrator is designated as the person who has oversight responsibility and control of a system or application, with the ability to add new users and change users' passwords and access rights. A good system of controls requires that the administrator's position be separate from the performance or monitoring of the Village's financial recordkeeping, including the Village's real property tax software. Where a proper segregation is not feasible, Village officials must implement adequate compensating controls. Further, to help ensure individual accountability over the financial records, no user accounts should be created without necessity, and each employee should use their own individual username to access software applications when processing and recording transactions.

The Village uses two different software packages from third-party vendors to handle the majority of its financial operations. One package records and processes financial transactions, including cash receipts, cash disbursements and employee payroll. The other package maintains real property tax records, including property assessments, exemptions and the collection and posting of payments received. These payments are periodically entered into the financial software in lump-sum entries.

Financial Software — The Treasurer is the financial system administrator, even though she is not independent of the financial recordkeeping functions. Therefore, the Treasurer inappropriately has the ability to add new users to the system, create and change user access rights and make or delete evidence of payments without restriction. We reviewed computer-generated check warrants and compared them to a selection of canceled check images[2] and found no inappropriate activity. However, we found five user accounts that the Treasurer was unable to provide an explanation for their necessity.[3] We observed audit logs for these five user accounts and found that there was no activity on these accounts.

Because of the improper assignment of administrative privileges and access rights and the existence of unnecessary user accounts, there is an increased risk that unauthorized changes to the accounting records, software security settings and user authorization privileges could occur and go undetected. This could lead to the loss of important financial data, interruptions to Village operations or the inappropriate use of Village assets.

Real Property Tax Software — We reviewed access rights and found that a Clerk has supervisor level access, which is similar to a system

[2] We reviewed 54 canceled checks, as indicated in Appendix C.

[3] Four of the five user accounts were duplicates of other user accounts in the financial software.

administrator account because it allows complete access to the tax software application. Therefore, the Clerk inappropriately has the ability to add, modify and delete property tax information[4] in the applications' modules and add, modify and delete user accounts. Further, Village employees used two generic user names to record collections of property taxes in the software application.

We reviewed a selection[5] of modifications made to real property assessments in the application software. Although we did not find any inappropriate activity, there is an increased risk that inappropriate changes could be made affecting the taxes paid or owed by individual property owners and that such activity could not be associated with an individual employee.

Disaster Recovery

A disaster recovery plan describes how Village officials will deal with potential disasters. Such disasters may include any sudden, unplanned catastrophic event (e.g., fire, computer virus or inadvertent employee action) that compromises the availability or integrity of the IT system and data. Contingency planning averts or minimizes the damage that disasters could cause to operations. Such planning consists of precautions to minimize the effects of a disaster so officials and staff will be able to maintain or quickly resume day-to-day operations. Typically, a disaster recovery plan involves an analysis of business processes and continuity needs, including a significant focus on disaster prevention. The plan should also address the roles of key individuals and be distributed to all responsible parties, tested periodically and updated as needed.

The Board has not adopted a comprehensive disaster recovery plan. Consequently, the Village does not have a plan that specifically addresses IT, that includes details on the records and data that are essential to preserve during a disaster or that designates alternate work locations. In the event of disaster, Village personnel have no guidelines or plan to minimize or prevent the loss of equipment and data or to recover data. Without a comprehensive disaster recovery plan, the Village could lose important financial data and suffer a serious interruption in Village operations.

Recommendations

The Board should:

1. Adopt policies and procedures to address internal user access, remote access, password security and management and data backups.

---

[4] This information includes the assessment values, exemptions, property descriptions and owner information.

[5] We reviewed 11 properties that had a decrease in the assessed value in 2014-15, as indicated in Appendix C.

2. Establish a policy to ensure that access to the IT system is provided only to specified persons and only based on the needs associated with their job functions. All generic user accounts should be removed, and administrative rights should be restricted to only those individuals who need them.

3. Adopt and distribute to all responsible parties a comprehensive disaster recovery plan to document the records and data that are essential to preserve during a disaster and identify alternate work locations. This plan should be periodically tested and updated.

Village officials should:

4. Designate an administrator who does not perform or monitor the Village's financial or property tax recordkeeping.

5. Develop written procedures to assign user access rights based on job duties. Where a proper segregation is not feasible, Village officials should implement adequate compensating controls.

APPENDIX A

RESPONSE FROM VILLAGE OFFICIALS

The Village officials' response to this audit can be found on the following pages.

THE HOOK MILL
ONE OF THE EARLY LONG ISLAND MILLS USED BY EARLY SETTLERS TO GRIND WHEAT, CORN AND OTHER GRAIN. BUILT IN 1806, IS STILL OPERATED. OPEN TO THE PUBLIC

VILLAGE OF EAST HAMPTON
Settled 1648 - Incorporated 1920
86 MAIN STREET
EAST HAMPTON, N.Y. 11937-2730
WWW.EASTHAMPTONVILLAGE.ORG
631-324-4150
FAX 631-324-4189
OFFICE OF

MAYOR

"HOME SWEET HOME"
DEDICATED TO THE MEMORY OF JOHN HOWARD PAYNE AND HIS FAMOUS SONG "HOME SWEET HOME". MAINTAINED BY THE VILLAGE AS A MUSEUM

October 14, 2015

Mr. Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788

RE: Village of East Hampton Information Technology Report of Examination
Response Letter to 2015M – 187

Dear Mr. McCracken:

Please allow this letter to serve as the Village of East Hampton's official response to the aforementioned report that covered the period of time from August 1, 2013–April 30, 2015. Also included in this response is the Village's Corrective Action Plan (CAP).

Policies and Procedures

The draft audit recommends the Village adopt a more comprehensive computer and information technology policy. The Village currently has an adopted Local Law concerning breach notification, acceptable computer use and email and internet usage policies. The Village intends to adopt at its October 16, 2015 Trustee Meeting, an updated Electronic Communications Policy (a copy which has already been provided to OSC staff) as per the draft audits recommendations concerning internal user access and security measures. The Village IT consultant currently performs multiple daily backups of Village data and its systems both on site and at an offsite location as well. The backup system is tested, minimum, on an annual basis. The Village will continue to perform these functions.

Network User Accounts

The draft audit alleges that Village officials improperly created generic user accounts on the Village's financial and real property tax software. As has been brought to the attention of OSC staff, the Village did not create these generic accounts (which the draft audit does properly state have never been accessed by any Village official or employee). The accounts were created by the software companies themselves as part of the file creation process. As such, so long as they are not needed for back up or any other IT function, the Village will eliminate the accounts.

The draft audit states that it is not ideal for one employee or official to have sole access to creating user accounts, and assigning appropriate user privileges to other employees. While it is crucial to the Village's financial operation that there is one official/employee that can perform these tasks, the Village will begin random user audits on these accounts to ensure the appropriate employee continues to assign needed users and their functions.

User Access to Application Software

The draft audit makes recommendations regarding user access for the Village's two main software programs: the financial (budget) software and the real property tax software.

With regard to the financial software, again the draft audit recommends that one official/employee should not have the level of access that she currently has. Again, since it is critical that the employee retain that right to said access level, the Village will begin random audits of user access to ensure continued compliance. Also, as previously indicated, the generic user accounts were never accessed and were created by the software company itself, not the Village.

The Village's real property tax software creates a similar issue, according to the draft audit, that a single employee has supervisor level access to the software program. Again, as indicated to OSC staff, it is imperative to the function of the employee's job, that said access be preserved. In order to provide a compensating control, the Village has added another employee to the program with the same access level and they will be able to perform user audits to ensure the employee continues to properly use the software program.

The Village does maintain two generic accounts for the program when taking tax payments and when they are entered into the system by Village employees. The Village will begin initialing payments by the employees who take the payments. The draft audit alleges that there may be an increased risk for inappropriate changes to be made to taxes owed in the

program because of the generic accounts however, the Village disputes this statement. The software program does not allow a user to alter the amount owed once it is in the system and the system does not allow partial payments to be entered. Therefore, an employee must enter the appropriate amount owed making it impossible to change the amount owed on a parcel at the time a payment is made. Also, the Village does monthly proofs to verify the amount of taxes billed, payments received and the bills that are outstanding. As such, the real property tax system policies and procedures followed by the Village are efficient and are managed very closely to ensure payments are appropriate.

See Note 1 Page 13

The draft audit does properly indicate that Village staff has not engaged in any inappropriate access and that all audited claims and programs were correct for both software programs.

Disaster Recovery Plan

The draft audit recommends the Village adopt a formal disaster recovery plan to deal with potential disasters or disruptions to the Village's IT system. The Village will adopt formal written polices to that effect. As indicated earlier, the Village currently does backup onsite and offsite of all of its systems multiple times daily. Should a disruption or disaster occur, due to the offsite backup capabilities already in place, the Village would be able to recoup and recover programs and systems and estimates a two to seven day timeframe to get back and running. The Village does testing of its backup systems at minimum, on an annual basis, and will continue to do so.

The Village of East Hampton thanks the Office of the State Comptroller for its assistance and due diligence throughout this process.

Sincerely yours,

Paul F. Rickenbach, Jr.

APPENDIX B

OSC COMMENT ON THE VILLAGE'S RESPONSE

Note 1

Although the real property tax software may require the amounts entered to agree with the amounts owed for specific parcels, the access controls do not mitigate the risk associated with generic user accounts and inappropriate administrative access rights.

APPENDIX C

AUDIT METHODOLOGY AND STANDARDS

The objective of our audit was to determine if computerized financial data and assets were properly safeguarded from August 1, 2013 through April 30, 2015. To achieve our audit objective and obtain valid audit evidence, we performed the following procedures:

- We reviewed the Village's existing policies and procedures.

- We interviewed Village officials, employees and the IT vendor to gain an understanding of the IT environment and internal controls in place.

- We obtained a list of all 52 users of the Villages network to determine if there were generic user accounts, if all users were active employees and if there was an explanation for all employee and non-employee user accounts.

- We reviewed the financial software user permission report to determine if there were excessive or generic user accounts.

- We obtained a list of all users of the financial software and their access rights to determine if users had excessive user permissions and if their access to the financial software was consistent with their job duties.

- We reviewed audit logs for five user accounts for the audit period to determine if there was any inappropriate activity.

- We reviewed 54 of the 213 canceled checks included in the June 2014 bank statements totaling $42,006. We compared the check images to the Board-approved check warrants, we ensured that computer-generated check warrants matched the check images and we reviewed the warrants to ensure there was an explanation for each check.

- We reviewed the real property tax software user permission report to determine if there were excessive or generic user accounts.

- We obtained a list of all users of the real property tax software and their access rights. We determined if users had excessive user permissions and if their access to the software was consistent with their job duties.

- We reviewed all 11 properties that had a decrease in assessed value over $3,000 in the 2014-15 fiscal year totaling $81,575. We compared the assessment changes made in the real property tax software to the property deeds maintained by the Town of East Hampton.

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 D

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 E

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

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy 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