Office of the New York State Comptroller

Division of Local Government
& School Accountability

Town of Saugerties

Information Technology

Report of Examination

Period Covered:

January 1, 2014 — February 28, 2015

2015M-117

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

August 2015

Dear Town 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 Town Board 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 Town of Saugerties, 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 Town of Saugerties (Town) is located in Ulster County and has a population of approximately 20,000 residents. The Town Supervisor (Supervisor) serves as the Town's chief executive officer. The Town Board (Board) comprises the Supervisor and four Board members. The Board is the legislative body responsible for managing Town operations including security over the information technology (IT) environment. The Town's 2015 general fund budget was approximately $8.23 million, funded primarily by real property taxes.

The Town contracts for IT services with an independent contractor. The contractor's duties include performing all significant maintenance and hardware installations, and providing technical support and expert advice on the upgrade of the entire IT environment. The Town uses computerized applications to perform essential tasks including processing financial information, Police and Town Clerk services, and Building Department transactions. The Town has approximately 77 computers, 24 laptops and two main servers.

Objective

The objective of our audit was to determine whether the Town's IT assets were adequately safeguarded. Our audit addressed the following related question:

- Are internal controls over IT appropriately designed and operating effectively?

Scope and Methodology

We examined the Town's internal controls over IT systems for the period January 1, 2014 through February 28, 2015. We extended our review of data extracted from the Town's computers and networks through May 6, 2015. Our audit disclosed areas in need of improvement concerning the oversight of IT operations. Because of the sensitivity of some of this information, certain vulnerabilities are not discussed in this report but have been communicated confidentially to Town officials so they can 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 Local Officials and Corrective Action

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

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 the 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 Town Clerk's office.

Information Technology

The use of information technology (IT) affects the fundamental manner in which transactions are initiated, recorded, processed and reported. The extent to which computer processing is used in significant accounting applications, as well as the complexity of that processing, determines the specific risks that IT poses to the Town's internal controls. The Town's widespread use of IT presents a number of internal control risks that must be addressed. Those risks include, but are not limited to, unauthorized access to data, unauthorized changes to data in master files and potential loss of data. Town officials must design internal controls to safeguard computerized data from loss or misuse.

The Board needs to improve internal controls to effectively protect the Town's computer system and data. Specifically, the Board needs to review user access and restrict administrative rights to those who need such rights to perform their jobs. The Board also has not provided Town personnel with a copy of the acceptable computer use policy. Furthermore, the Board has not developed computer security and disaster recovery plans, and has not established a breach notification policy or a comprehensive inventory policy for all hardware and software. As a result of these weaknesses, there is an increased risk of loss of critical data and interruptions to Town operations.

User Access

An important component of internal controls over computer systems and data includes policies and procedures for granting, revoking and modifying individual access rights. Access controls should be based on the principle of least privilege, which maintains that users should have the most limited access rights possible to complete their authorized duties. Administrator rights are considered elevated privileges because they allow users to create, delete and modify files, folders or settings. Generally, an administrator is designated as the person who has oversight and control of a system or application with the ability to add new users and change users' passwords and access rights. All user accounts should be assigned to specific users, and any inactive accounts should be deleted or disabled from the system.

Users with administrative rights have complete control over their local workstation. Users could perform actions that would significantly impact the safety and security of the computer and data including installing unauthorized software and gaining unauthorized access to all file shares or data resources. According to the Town's IT consultant, all users have administrator rights to their computers. We

verified this on nine of the computers[1] that we manually examined during our onsite testing.

There are 94 user accounts on the Town's server and 96 user accounts on the Police Department's server. We found 51 inactive user accounts (25 on the Town's server and 26 on the Police Department's server); nine[2] of these inactive users are no longer employed by the Town and should be disabled. Of the remaining 42 inactive accounts, 20 are generic user names, meaning the account is not associated with a unique individual (based on the common name defined on the account). The use of generic accounts can prevent the Town from tracing a suspicious activity to a specific individual, thus presenting difficulties in holding the responsible user accountable for any inappropriate actions. The remaining 22 accounts have not had any activity from December 2008 through February 2015 (60 days from April 1, 2015, the most recent date reviewed).

The Board does not review user access on an ongoing basis and needs to restrict administrative rights to those who need them to perform their jobs. It is anticipated that when the Town purchases a new server, a new domain will be constructed. At that time, Town officials plan to review all current users and access will be granted based on current job responsibilities.

When access to computers and applications is not controlled, accountability is compromised. Furthermore, without reviewing and updating authorized users, the risk of the system being compromised by unauthorized parties, without detection, increases.

Policies and Procedures

Policies and procedures over IT are part of the internal control system and provide criteria and guidance for computer-related operations. Effective protections of computing resources and data include the adoption of an acceptable use policy that informs users about appropriate and safe use of Town computers, a security plan which identifies potential risks and how to reduce system threats, a disaster recovery plan with guidance for minimizing loss and restoring operations in the event of a disaster and establishing a breach notification policy to ensure that employees are adequately prepared to notify affected individuals if their private information is compromised. The Board should periodically review and update these policies as necessary to reflect changes in technology and the Town's computing environment. Computer users also need to be aware of

[1] We chose one computer from every department with the exception of the Highway Department. The Highway Department's computers were upgraded on April 1, 2015.

[2] Eight were former employees and one is the former IT consultant.

security risks and be properly trained in practices that reduce the internal and external threats to the network.

Acceptable Use – An acceptable use policy defines the Board's intended use of equipment and computing software and the security measures that are designed to protect the Town's system and confidential information. The policy should address, but not necessarily be limited to, the acceptable use of the Internet and email, password security, access to and use of confidential information, and the installation and maintenance of software on Town desktops and laptop computers.

Although the Town has established an acceptable use policy, Town officials were not able to demonstrate that users were aware of the policy. The acceptable use policy has an acknowledgment page that employees must sign to indicate they understand and will comply with the policy. We reviewed the computer activity for nine users. Town officials could not provide us with a signed acknowledgement of the acceptable use policy for any of these users. Town officials did not realize that this acknowledgement was not on file in the Town office. Without the users' awareness of such a policy, there is no requirement in place to ensure that computers are used in an appropriate and secure manner, which could potentially expose the Town to malicious attacks or compromise systems and data.

Further, of the nine users reviewed, we found evidence of personal use on two computers, and three computers had personal websites book marked in their favorites. The users visited sites that had no Town business purpose, including sites for social networking, personal email, motorsports, shopping and entertainment.

Computer Security – Computer users need to be aware of security risks and be properly trained in practices that reduce the internal and external threats to the system. It is essential for Town officials to develop a written security plan to document the process for evaluating and assessing security risks, identify and prioritize potentially dangerous issues, and document the process for discussing and determining solutions. An effective IT security plan also includes provisions for the monitoring of computer use to ensure compliance, as well as provisions for policy enforcement. Additionally, the security plan should require that only Town-owned devices remain on the network to ensure adequate control of the Town's network security. The implementation of effective IT policies and procedures facilitates the protection of computerized data resources from internal and external threats.

The Board has not developed a written computer security plan. The lack of a formal security policy leaves the Town vulnerable to the risks associated with individual use, including viruses, spyware and other forms of malicious software that could potentially be introduced through non-work-related websites or programs. The Town's IT assets are more susceptible to loss or misuse when users are not aware of security risks and practices necessary to reduce those risks.

Disaster Recovery – A disaster recovery plan is intended to identify and describe how Town 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 is used to avert or minimize the damage and impact that disasters would cause to operations. Such planning consists of the precautions to be taken to minimize the effects of a disaster so officials and responsible 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, periodically tested and updated as needed.

The Board has not adopted a comprehensive disaster recovery plan to address potential disasters. Town officials told us that they trust the IT contractor and his informal plan for disaster recovery. Consequently, in the event of a disaster, Town personnel have no guidelines or plan to follow to help minimize or prevent the loss of equipment and data or to appropriately recover data. Without a comprehensive disaster recovery plan, the Town could lose important financial data and suffer a serious interruption in Town operations.

Breach Notification Policy − An individual's private and financial information, along with confidential business information, could be severely impacted if the Town's computer security is breached or data is improperly disclosed. New York State Technology Law requires the Town to establish an information breach notification policy. Such a policy should detail how the Town would notify individuals whose private information was, or is reasonably believed to have been, acquired by a person without a valid authorization. It is important for the disclosure to be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Town officials informed us that the Board had not adopted a breach notification policy. We discussed this weakness with the former

Supervisor in a prior audit report issued in 2012.[3] Town officials did not implement any of the recommendations in that report and did not prepare and submit a corrective action plan as required.

Security Awareness Training − An important way to communicate IT security expectations to network users is by providing IT security awareness training. IT awareness training is intended to assist individuals with recognizing IT security concerns and then responding appropriately. Creating security awareness through training also helps to ensure that everyone understands his or her individual responsibilities.

Town employees were not provided with training to ensure they understood security measures designed to protect the Town's network. Employees' lack of training makes the Town's IT assets more vulnerable to loss and misuse.

Inventory

A good system of internal controls includes policies and procedures that are designed to ensure that employees record and maintain an inventory of computer and technology equipment and software. A detailed inventory record should include a description of each item, including make, model and serial number; the name of the employee to whom the equipment is assigned, if applicable; the physical location of the asset and relevant purchase information including acquisition date. It is important that inventory records be periodically checked and kept up to-date with new acquisitions, disposals and current condition of these assets. Policies and procedures help to reduce the risk of loss, theft, misuse and obsolescence. Maintaining inventory records helps safeguard assets and provides a means of planning for future replacement and a reference for the asset's location.

The Town does not maintain a complete inventory of computer and technology equipment; the inventory records that the Town maintains lack key identifying information. The IT consultant provided us with a listing of Town Hall computers that included location, the assigned user and the operating system. However, this listing lacked the make, model, serial number and acquisition cost and date. We also obtained various IT inventory lists from department heads for the Building, Parks and Police Departments; these inventory lists also lacked identifying information.

In addition, the Town does not have a software inventory other than each computer's operating system. Town officials do not conduct audits or formal reviews of software installed. Of the nine computers

[3] *Town of Saugerties, Internal Controls Over Selected Financial Activities*, 2011M-283, May 2012

reviewed, we found two suspicious software programs installed. These programs are adware and were probably inadvertently downloaded while downloading other free software. Furthermore, we found that the support for the Town's two main servers will end in July 2015. The Town is replacing the Town Hall server prior to that; however, the Police Department server is not in this year's budget and will not be replaced until next year. The IT consultant stated the Town will contract with the vendor for the additional support until the Police Department's server is replaced.

The Town has had recent administration changes and the new administration has made upgrading the Town's IT environment a priority, including compiling inventory lists for the Town's computer assets. Without an accurate inventory of computer and technology equipment, Town officials cannot be assured that these assets are adequately accounted for and protected from loss, theft, misuse and obsolescence. Further, in the event of a disaster, the Town would be unable to provide the insurance company with an accurate list of assets, and Town officials would be unaware of what they needed to replace.

Recommendations

The Board should:

1. Limit the administrative access rights to those individuals that have oversight and control of a system or application, and review those rights on an ongoing basis. All user accounts should be assigned to specific users and any inactive accounts should be deleted or disabled from the system.

2. Provide Town personnel who use computers a copy of the acceptable use policy and retain a signed copy of the acknowledgement page to ensure the users' understanding and their responsibilities to the Town policy.

3. Adopt IT policies and procedures related to:

    a. Computer security.

    b. Disaster recovery.

    c. Breach notification.

4. Ensure all network users receive IT security training.

5. Establish a comprehensive inventory policy that defines procedures for maintaining a complete, comprehensive

inventory listing for all hardware and software; updating inventory records for all new purchases as they occur and relocating assets (if necessary). The Board also should formalize a policy to perform reviews of the Town's computers and compare results to the Town's inventory list.

APPENDIX A

RESPONSE FROM LOCAL OFFICIALS

Town officials' response to this audit can be found on the following pages. Town officials included comments regarding findings we had communicated confidentially to them. Because of the sensitivity of this information, we did not include it in the report. Town officials also attached updated policies and server replacement information with their response. However, their response contained sufficient information to indicate their intentions. Therefore, we did not include these attachments in the final report.

TOWN OF SAUGERTIES

4 HIGH STREET, TOWN HALL
SAUGERTIES, NEW YORK 12477

TEL. (845) 246-2800 FAX. (845) 247-0355

GREG L. HELSMOORTEL
SUPERVISOR
FRED COSTELLO, JR.
DEPUTY SUPERVISOR

MEMBERS OF TOWN BOARD
JAMES J. BRUNO
WILLIAM M. SCHIRMER
LEEANNE THORNTON

July 28, 2015

Gabriel Deyo-Deputy Comptroller
NYS Comptroller's Office
110 State St.
Albany, NY 12236

Dear Deputy Comptroller Deyo,

The Town of Saugerties offers the attached responses/remedies (from the town's in-house IT consultant) to the findings reported in the audit regarding the town's information technology for the period covering 1-1-14 thru 2-28-15 and to your letter of June 2015 regarding [redacted]

The town has and will continue to institute corrective actions to improve its information technology as described/encompassed in the future projects & goals and several policies that are also attached.

If you have any questions concerning our response and recommendations please feel free to contact my office at (845) 246-2800 ext. 345.

Sincerely,

Greg Helsmoortel, Supervisor

cc: [redacted]
IT Consultant
Town Board Members

New York State IT Final Audit Response

Report Prepared by: Nicholas Monaco – IT Consultant for the Town of Saugerties

July 25, 2015

This report will be addressing the recommendations by the New York State Office of the Comptroller.

1. Limit the administrative access rights to those individuals that have oversight and control of a system or application, and review those rights on an ongoing basis. All user accounts should be assigned to specific users and any inactive accounts should be deleted or disabled from the system.

   This recommendation will be complied upon by the installation of the new town server which has already been purchased and it due to be installed and operational by the end of August 2015

2. Provide Town personnel who use computers a copy of the acceptable use policy and retain a signed copy of the acknowledgement page to ensure the users' understanding and their responsibilities to the Town policy

   The town is planning an in-service training seminar for all town employees in September 2015 that will address new policies and procedures and the acceptance of the policies. A signed acknowledgement of the policies and procedures will be obtained from the employees and maintained by the town. Also to be included will be IT Security training.

3. Adopt IT policies and procedures related to:
   a. Computer security
   b. Disaster recovery
   c. Breach notification

   Policies for the following have been written and will be adapted by the town as soon as prudent, according to town policy adaptation procedures. (see attached policies)

   a. Computer Security
   b. IT Disaster Recovery
   c. IT Breach Notification
   d. Password Complexity

4. Ensure all network users receive IT security training.

   Addressed in recommendation number 2

5. Establish a comprehensive inventory policy that defines procedures for maintaining a complete, comprehensive inventory listing for all hardware and software; updating inventory records for all new purchases as they occur; and relocating assets (if necessary). The Board also should formalize a policy to perform reviews of the Town's computers and compare results to the Town's inventory list.

   The town shall be hiring a part time employee to establish a complete and comprehensive inventory listing for all hardware and software in the town. This inventory shall be completed by assigning an inventory control number to each asset. A database of said inventory will be maintained from herein and all purchases and dispositions of IT equipment will be recorded. The database shall contain the following, but not limited to:

   Date/Make/Model/Serial#/Inventory Control#/Location/Date purchased

   Purchase price/Purchased From/Disposition Date/Manor of Disposition.

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

The objective of our audit was to examine the IT controls over the Town's electronic data and computer resources. To achieve our audit objective and obtain valid evidence, we performed the following procedures:

- We interviewed Town officials and the contracted IT consultant to obtain an understanding of the Town's IT operations.

- We inquired as to policies and procedures related to acceptable use, user accounts, security and disaster recovery plans, breach notification and security awareness training.

- We examined nine computers by running audit software and examined specific activities such as Internet use, cookies and Internet history.

- For our sample of computers chosen, we chose one computer from every department with the exception of the Highway Department. The Highway Department's computers were upgraded on April 1, 2015.

- We inquired to determine if Town officials maintained lists of computers, IT assets, applications, system users or access abilities.

We conducted this performance audit in accordance with generally accepted government auditing standards (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
Nathaalie N. Carey, 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