



Town of Troupsburg Internal Controls Over Information Technology

Report of Examination

Period Covered:

January 1, 2011 — August 16, 2012

2012M-200



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	2
INTRODUCTION	3
Background	3
Objective	3
Scope and Methodology	3
Comments of Local Officials and Corrective Action	4
INFORMATION TECHNOLOGY	5
Acceptable Use	5
Breach Notification	6
Computer Security	6
Data Backup	7
Disaster Recovery Plan	7
Recommendations	8
APPENDIX A Response From Local Officials	9
APPENDIX B Audit Methodology and Standards	12
APPENDIX C How to Obtain Additional Copies of the Report	13
APPENDIX D Local Regional Office Listing	14

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

December 2012

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 Town of Troupsburg, entitled Internal Controls Over 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 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 Troupsburg (Town) is located in Steuben County and has a population of approximately 1,300. The Town provides various services including highway maintenance and improvement, snow removal, public water and sewer, and general government support. These services are funded primarily by real property taxes, sales tax, and State aid. Budgeted appropriations totaled approximately \$1 million for the 2012 fiscal year.

The Town is governed by an elected five-member Town Board (Board) comprising the Town Supervisor (Supervisor) and four Board members. The Board is responsible for the overall management of the Town's operations and finances. The Board develops policies and procedures, and enacts laws, ordinances, and resolutions to assist them in their oversight responsibilities. As the Town's chief fiscal officer, the Supervisor is responsible for receiving, disbursing, and safeguarding cash and maintaining a record of such cash transactions. The Supervisor is assisted with these duties by the bookkeeper.

The Town uses five stand-alone desktop computers to process and store financial and non-financial data, and to provide email communications and Internet access to Town officials and employees. The bookkeeper also uses his personal laptop computer for Town financial and non-financial data. Day-to-day management of the Town's computer system has been the responsibility of the bookkeeper.

Objective

The objective of our audit was to assess internal controls over the Town's information technology (IT) environment. Our audit addressed the following related question:

- Did the Board provide adequate internal controls over the Town's information technology to ensure that the Town's computerized data and assets are safeguarded?

Scope and Methodology

We examined the Town's internal controls over IT for the period January 1, 2011 to August 16, 2012

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 they planned to initiate 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 Town Board to make this plan available for public review in the Town Clerk's office.

Information Technology

The Board is responsible for creating an appropriate internal control environment to protect IT computer equipment, software and data. Computer systems and electronic data are a valuable resource that Town officials rely on for making financial decisions, processing transactions, keeping records, and reporting to State and Federal agencies. Large amounts of information and data related to finances, taxes, water and sewer rents, payrolls, personnel, and building permits are stored on the IT system. Risks, such as unauthorized access, increase the risk that computerized equipment could be damaged or data misused, lost, or corrupted without detection. Even small disruptions can require extensive time and effort to evaluate and repair. It is therefore essential for the Board to establish policies and procedures to help ensure appropriate computer use, breach notification and data backup, and developing written security and disaster recovery plans to help prevent the loss of computerized data and for resuming operations in the event of a disaster.

The Board has not established adequate internal controls over the Town's IT system to ensure the Town's computerized data and assets are safeguarded from internal and external threats. The Board has not established policies and procedures related to acceptable use, data backup and computer security, and the Board has not adopted a disaster recovery plan to address potential disasters. In addition, the Board has not adopted a data breach policy as required by law. While IT policies do not guarantee the safety of the Town's IT system or the electronic information it has been entrusted with by taxpayers, customers, employees and others, the lack of policies significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use. This leaves the Town vulnerable to risks associated with personal use, including computer viruses and spyware that could potentially be introduced by accessing non-work-related websites or downloading unauthorized programs.

Acceptable Use

Good internal controls over computerized data include an acceptable use policy that informs users about proper use of Town computers and requires the monitoring of computer usage to ensure compliance. An acceptable use policy defines the Board's goals for the use of equipment and computing systems, and the security measures to protect the Town's resources and confidential information. The policy must address the acceptable use of email accounts, Internet access, and the installation of software on Town computers. It is important that the policy include provisions for enforcement, and that system users provide written acknowledgement that they are aware of, and abide by, the policy.

The Board has not adopted an acceptable use policy to ensure the security of the IT system. Without comprehensive policies that explicitly convey the appropriate use of the Town's IT equipment, Town officials cannot be assured that users are aware of their responsibilities and there are no consistent standards for which users are held accountable.

Breach Notification

New York State Technology Law requires towns to establish an information breach notification policy. Such a policy helps to ensure that affected residents or employees are notified when their 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.

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, Town officials and employees may not understand or be prepared to fulfill their legal obligation to notify affected individuals.

Computer Security

It is essential for Town officials to develop a formal, written security plan to document the process for evaluating and assessing security risks, to identify and prioritize potentially dangerous issues, and to document the process for discussing and determining solutions. The plan should establish a framework for preventing possible exposure to risk, and include policies and procedures on specific security areas such as the use of unsecure or unprotected storage and personal computing devices, controls over sensitive data, and audit logs (automated trails of user activity).

Town officials have not developed a written security plan to document any processes or procedures that may already be in place or to institute specific controls to ensure that sensitive data is properly secured and stored. Town officials have not developed policies for the use of personal computing devices (such as thumb drives, or personal laptops). Because of the failure to address potential security weaknesses and develop a written, enforceable security plan, areas that could be at risk may have been overlooked, and informal policies and procedures to control risk may be inconsistently applied or ineffective. For example, the bookkeeper often uses his own personal computer to work offsite and record the Town's financial transactions. He backs up the data from his personal computer to a personally owned unsecured thumb drive and then restores the data to the Town's computers and vice versa. Therefore, access to the Town's financial

information is unrestricted, which increases the risk that personal, private and sensitive information could be misused without specific individuals being held accountable, and data could be intentionally or unintentionally deleted or corrupted. Finally, personally owned thumb drives and other computing devices may unintentionally transfer malware and worms¹ onto the Town's computers.

Data Backup

One of the basic rules in using computers is to protect data by backing up files regularly. Even the most reliable computer is apt to break down eventually. Data stored on computers should be backed up (a duplicate copy of information made) on a routine basis to enable it to be restored in the event of loss. Many professionals recommend that you make two, or even three, backups of all your files. In addition, the back-up copy of data should be stored at a secure offsite location and periodically tested to ensure that the data could actually be restored.

The Board has not established policies or procedures for the backup of Town information, including the financial data. As a result, the Town Clerk is not backing up financial and non-financial data that resides on the town issued computer at the Town hall. Although the bookkeeper creates a backup of the Town's financial data² on a monthly basis, the data is stored on an unsecured thumb drive. Furthermore, the Town does not have a formal process in place to periodically test whether it could restore data from the backups. Therefore, there is no assurance that backups will work.

Disaster Recovery Plan

A disaster recovery plan should be in place to prevent loss of the computer equipment and data and procedures for recovery in the event of a loss. A disaster recovery plan is intended to identify and describe how Town officials plan to deal with potential disasters. Such disasters may include any sudden, catastrophic event (e.g., fire, computer virus, or deliberate 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 that disasters would cause to operations. Such planning consists of the precautions 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, disaster recovery planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention. The plan should

¹ Malware, or malicious software, consists of programming designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, or otherwise cause damage. A computer worm is a self-replicating malware computer program, which uses a computer network to send copies of itself to other computers on the network.

² The financial data consists of transactions recorded in the Town's financial accounting and water/sewer billing software programs.

address the roles of key individuals, be distributed to all responsible parties, periodically tested, and updated as necessary.

The Board has not adopted a disaster recovery plan. 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 guidance on how to implement disaster recovery procedures. The lack of a disaster recovery plan could lead to loss of important financial data along with a serious interruption to Town operations, such as not being able to process checks to pay vendors or employees.

Recommendations

1. The Board should adopt formal IT policies pertaining to acceptable use, breach notification, and data backup, and implement procedures to effectively safeguard and monitor the Town's IT resources.
2. The Board should develop a formal, written security plan and ensure that it is communicated to, and understood by all appropriate personnel.
3. The Board should ensure that backups of Town information are stored at an environmentally and physically secure offsite location. This data should be periodically tested to verify that it is capable of restoring the Town's system.
4. The Board should establish a formal disaster recovery plan that address the range of potential threats to the Town's IT systems and data, and provides guidance necessary to maintain Town operations or restore them as quickly as possible in the event of a disaster. This should be distributed to all responsible parties, periodically tested, and updated as necessary.

APPENDIX A

RESPONSE FROM LOCAL OFFICIALS

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

TOWN OF TROUPSBURG

P.O. BOX 117

TROUPSBURG, NY 14885

SUPERVISOR

Frederick G. Potter

HIGHWAY SUPERINTENDENT

Ronald D. Button

TDD Number 1-800-662-1220

Phone Number 607-525-6403

Fax Number 607-525-6409

TOWN CLERK

Paula M. LeBarron

TOWN JUSTICE

Michael D. Whitfield

November 20, 2012

Edward V. Grant, Jr., Chief Examiner

The Powers Building

16 West Main Street, Suite 522

Rochester, NY 14614-1608

Dear Mr. Grant:

This is my response to the preliminary draft findings of the NYS Office of the State Comptroller's Report of Examination of the Town of Troupsburg for the period of January 1, 2011 to August 16, 2012, report #2012M-200. As with past audits, we view an audit to be a helpful tool to improve our operations. Furthermore it serves to assure the public that the records are accurate and that no fraud has occurred. It also serves to help identify areas of risk to which the town may be exposed.

We are pleased to learn that the accounting records were found to be accurate and complete and that there were no issues of concern with the town officials. Because of this, the focus of your audit was on risk assessment. Your assessment determined that the area most at risk is internal controls over information technology (IT). The areas that need to be addressed are stated to be as follows:

1. Acceptable use policy
2. Breach notification policy
3. Computer security plan
4. Data backup plan
5. Disaster recovery plan

Upon review of the draft audit report, we are in agreement with the findings. IT security is an area we had been addressing prior to the audit but specific policies or plans were not in place for doing so and as we learned from the draft report, risk areas existed beyond the scope of our efforts.

On behalf of the Troupsburg Town Board, I want to thank you for the opportunity to respond to the draft Report of Examination. Please note that as areas of concern were brought to our attention during the audit, we began addressing them immediately such as securing hardware and software. Research to find examples of acceptable policies and plans to address the areas listed in the report was started. We will use these examples to develop and adopt policies and plans that are appropriate to our needs and address the areas noted in the draft report.

This institution is an equal opportunity provider and employer. To file a complaint of discrimination, write USDA, Director, Office of Civil Rights, 1400 Independence Ave., SW, Washington, DC 20250-9410 or call (800) 795-3272 (Voice) or (202) 720-6382 (TDD)

Upon the completion of this process, and within 90 days of receipt of the final report, a Corrective Action Plan will be submitted explaining how the plans and policies will address the areas of concern. The Corrective Action Plan will also detail how these plans and policies will be implemented that create an appropriate internal control environment to protect the town's IT computer equipment, software and data.

Sincerely,

Frederick G. Potter
Town Supervisor

This institution is an equal opportunity provider and employer. To file a complaint of discrimination, write USDA, Director, Office of Civil Rights, 1400 Independence Ave., SW, Washington, DC 20250-9410 or call (800) 795-3272 (Voice) or (202) 720-6382 (TDD)

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

Our overall goal was to assess the adequacy of the internal controls put in place by officials to safeguard Town assets. To accomplish this, we performed an initial assessment of the internal controls so that we could design our audit to focus on those areas most at risk. During the initial assessment, we interviewed Town officials, performed limited tests, and reviewed pertinent documents such as Town policies and procedures, Board minutes, and financial records and reports.

After reviewing the information gathered during our initial assessment, we determined where weaknesses existed, and evaluated those weaknesses for the risk of potential fraud, theft and/or professional misconduct. We then decided upon the reported objective and scope by selecting for audit the area most at risk. We selected information technology for further testing.

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

- We interviewed appropriate Town officials about policies and practices, and how policies and practices are communicated to employees.
- We observed the locations of the Town's computers.
- We reviewed the access rights to the Town's financial software.

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
Steven J. Hancox, 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,
Osego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE

Robert Meller, 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-Bufferalo@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
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

Christopher Ellis, 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