



Town of Ithaca Information Technology

Report of Examination

Period Covered:

January 1, 2015 – December 22, 2016

2017M-52



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	1
INTRODUCTION	2
Background	2
Objective	2
Scope and Methodology	2
Comments of Local Officials and Corrective Action	3
INFORMATION TECHNOLOGY	4
IT Policy	4
Security Awareness Training	5
Computer Hardware Inventory	5
Contingency Planning	6
Recommendations	7
APPENDIX A Response From Local Officials	8
APPENDIX B Audit Methodology and Standards	10
APPENDIX C How to Obtain Additional Copies of the Report	11
APPENDIX D Local Regional Office Listing	12

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

June 2017

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 Ithaca, 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 Ithaca (Town) is located in Tompkins County and has approximately 20,000 residents. The elected, seven-member Town Board (Board) is the legislative body responsible for managing Town operations. The Town Supervisor (Supervisor) is a member of the Board and serves as the Town's chief executive officer and chief fiscal officer. The Supervisor is generally responsible for the administration and supervision of the Town's day-to-day fiscal operations.

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

The Town provides various services to its residents, including street maintenance and improvements, snow removal, parks and recreation and general government support. The Town's 2017 budgeted appropriations totaled approximately \$25 million, funded primarily with real property taxes, water and sewer fees and sales tax.

Objective

The objective of our audit was to assess the Town's IT policies and procedures. Our audit addressed the following related question:

- Have Town officials taken action to identify and correct IT deficiencies?

Scope and Methodology

We examined the Board's oversight of IT assets and computerized data for the period January 1, 2015 through December 22, 2016. 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 Town officials.

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

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 Town Clerk's office.

Information Technology

The Town's IT system is a valuable and essential part of operations, used for accessing the Internet, communicating by email, processing and storing data and maintaining financial records and reports. IT controls are a critical mechanism for ensuring that the IT system is properly safeguarded. The Board is responsible for ensuring that the right IT controls are in place and are performing as intended. Since computing environments change over the course of time, the Board should periodically review and update IT controls.

Town officials have not identified and corrected all IT deficiencies. Town officials have sufficiently addressed some areas such as IT service contracts, anti-virus protection, patch management, online banking, wireless networks and physical controls. However, we found improvement opportunities in areas such as IT policies, security awareness training, computer hardware inventories and contingency planning. Implementing these improvements will reduce the risk that data, hardware and software systems may be lost or damaged or that Town operations will be interrupted.

IT Policy

Computer policies define appropriate user behavior and describe the tools and procedures to protect data and information systems, taking into account people, processes and technology throughout the organization. Town officials should develop policies to cover the complexities of their IT environment including breach notification; Internet, email and personal computer use; use of and access to PPSI, password security, wireless security, mobile computing and storage devices and online banking. As social media becomes a more prominent communication resource, it is important for Town officials to develop a policy to address the use of social media on the Town's network. Additionally, the IT policy should be periodically reviewed and updated as necessary.

The Town's IT policy addresses breach notification; Internet, email and personal computer use; use of and access to PPSI and social media use. However, it does not address password security, wireless security, mobile computing and storage devices or online banking. Although Town officials told us that the IT policy does not address password security because it is common knowledge among staff, they had no explanation for the other areas not included in the policy. While computer policies will not guarantee the safety of a computer system, a lack of appropriate policies significantly increases the risk that data, and hardware and software systems may be lost or damaged by inappropriate access and use.

Security Awareness Training

A well-informed work force is the strongest link in the chain to secure electronic data and computer systems. Entities cannot protect the confidentiality, integrity and availability of their data and systems without ensuring that users understand organizational IT security policies and their roles and responsibilities related to IT. While IT policies tell staff what to do, annual IT security awareness training provides them with the skills to do it.

Town employees, including the specialist, have not received sufficient IT security and awareness training during our audit scope. The specialist has not attended cybersecurity training since September 2014. The specialist told us employees have not received formal IT training because it has never been required. However, her job description requires she provide IT training to staff, and she has provided informal training through emails and posters. Although informal training is provided, there is no guarantee staff are reviewing emails and posters.

We reviewed the web history of three employees. We did not identify any PPSI exposed; however, we identified questionable Internet usage, such as employees visiting social networking, email and entertainment sites, potentially for non-business purposes, and performing other Internet research and browsing of a personal nature using the Town's IT assets.

While their policy allows limited personal use, without training and awareness, such use opens the door to potential unauthorized access and/or misuse and abuse, such as employees accessing adult entertainment or gaming websites, which are known to have malicious content and could potentially cause service interruptions. Without formal IT security training and awareness, the risk still exists that users will not understand their responsibilities, which puts the data and computer resources with which they have been entrusted at greater risk for unauthorized access, misuse or abuse. Protecting IT assets is especially important as the number of instances of people with malicious intent trying to harm computer networks or gain unauthorized access to information through viruses, malware and other types of attacks continues to rise.

Computer Hardware Inventory

Organizations should maintain detailed, up-to-date inventory records for all computer hardware. The information for each piece of computer equipment should include a description of the item including the 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 or lease information including the acquisition date.

While the Town has a hardware inventory, it is not a detailed and up-to-date record for all computer hardware. We examined the computer hardware inventory which included 116¹ items, and found that 37 items, or 32 percent, were missing at least one of the following: the make, model, serial/service tag number or name of the employee they were assigned to, and the physical location was not documented for any of the 116 items.

The specialist told us the hardware inventory is incomplete because she assigned this work to an intern, and it was never finalized. While the inventory was, for the most part, complete, the failure to maintain detailed and up-to-date hardware inventory records exposes valuable assets to an increased risk of loss, theft or misuse.

Contingency Planning

A contingency plan describes how to 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 consists of the precautions to be taken, such as backup procedures, to avert or minimize the effects of a disaster and maintain day-to-day operations. Typically, a contingency plan involves an analysis of IT business processes and continuity needs, including a significant focus on service interruption. The plan should also address the roles of key individuals and be distributed to responsible parties, tested periodically and updated.

Town officials have established a written IT contingency plan, but it is not sufficient. Although Town officials have procedures to sufficiently backup data and an emergency preparedness plan, they have not established written data backup policies and the emergency plan does not specifically include IT procedures to maintain day-to-day operations such as the preservation of records and data during a disaster and alternate work locations. Based on discussions with the specialist, even the plan that is in place, while inadequate, has not been tested and has not been reviewed or revised since 2012.

The specialist indicated they were not aware that the plan was not sufficient and that it had not been reviewed or revised. As a result, in the event of disaster, Town personnel have no guidelines or plan to minimize or prevent the loss of equipment and data. Therefore, the Town could lose important financial data and suffer a serious interruption in Town operations.

¹ The list contained 53 computers, 38 monitors and 25 printer/copier/scanners.

Recommendations

The Board, with the assistance of the specialist, should:

1. Update the IT policy to address password security, wireless security, mobile computing and storage devices and online banking. Additionally, the policy should be periodically reviewed and updated as necessary.
2. Require all staff receive formal IT security and awareness training at least annually.
3. Ensure hardware inventory listings included the make, model and serial number, the name of the employee they are assigned to and the physical location.
4. Prepare an IT contingency plan that specifically addresses backup policies and procedures to maintain day-to-day operations such as the records and data to preserve during a disaster and alternate work locations. This plan should be tested, reviewed and updated as necessary to ensure it meets organizational needs.

APPENDIX A

RESPONSE FROM LOCAL OFFICIALS

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



TOWN OF ITHACA

215 N. Tioga Street, Ithaca, N.Y. 14850
www.town.ithaca.ny.us

TOWN SUPERVISOR 273-1721 x 125
FAX (607) 273-1704

June 12, 2017

H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building, Room 1702
44 Hawley Street
Binghamton, NY 13901-4417

Dear Mr. Eames:

I have discussed the Draft Town of Ithaca Information Technology Report of Examination for the period January 1, 2015 – December 22, 2016 (# 2017M-52) with the Ithaca Town Board, and we have no comments to add or corrections to make. The Report and recommendations seem reasonable to us, and it was a pleasure working with your staff. Thank you.

Sincerely,

William D. Goodman,
Town Supervisor

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

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

- We interviewed Town officials and employees to gain an understanding of the IT environment, internal controls and IT security training provided.
- We reviewed the Town's policies, technology plan and Board minutes for existing IT policies and procedures.
- We reviewed the Town's IT service contracts to determine whether they contained the proper components and established measurable targets of performance.
- We interviewed Town officials and observed employees' computers to determine whether adequate controls were in place regarding access, online banking, wireless networks and computer resources.
- We used audit software to analyze information on the Town's server and selected a sample of three computers to determine whether Internet usage was appropriate. We selected the specialist's computer because she has administrative access and total control over all computers. We selected the human resources manager's computer because she has administrative access and maintains PPSI. We selected the bookkeeper's computer because she performs online banking and has access to the financial software.
- We reviewed the Town's hardware inventory to determine whether it was detailed and up-to-date.
- We reviewed the Town's contingency plan and back-up procedures to determine whether they were sufficient.

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-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
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