



Town of Windsor Information Technology

Report of Examination

Period Covered:

January 1, 2015 — December 27, 2016

2017M-44



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	2
INFORMATION TECHNOLOGY	4
Acceptable Use Policy	4
Data Backup	4
Disaster Recovery Plan	5
Breach Notification Policy	5
Security Awareness Training	6
Server Location	6
Recommendations	6
APPENDIX A Response From Local Officials	8
APPENDIX B Audit Methodology and Standards	11
APPENDIX C How to Obtain Additional Copies of the Report	12
APPENDIX D Local Regional Office Listing	13

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

May 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 Windsor, 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 Windsor (Town) is located in Broome County. The Town Board (Board) is composed of the Town Supervisor (Supervisor) and four Board members. The Board is the legislative body responsible for managing operations, including ensuring security over the Town's information technology (IT) environment. The Supervisor serves as the Town's chief executive officer, chief financial officer and Information Systems Director. The Town's 2017 general fund budget was approximately \$880,000, funded primarily by real property taxes.

The Town contracts with Broome County for maintenance, support and access of its IT environment. The Town uses computerized applications to perform essential tasks including processing financial information. The Town has approximately 14 computers and one server.

Objective

The objective of our audit was to review the Town's IT controls. Our audit addressed the following related question:

- Do Town officials adequately safeguard personal, private and sensitive information on the Town's server and in the financial system?

Scope and Methodology

We examined the controls over IT for the period January 1, 2015 through December 27, 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 and indicated they planned to take 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 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

Computerized data is a valuable resource that Town officials rely on to make financial decisions and report to State agencies. If the computers on which this data is stored fail or the data is lost or altered, either intentionally or unintentionally, the results could range from inconvenient to catastrophic. Even small disruptions can require extensive time, effort and expense to evaluate and repair.

It is important that Town officials adopt a comprehensive IT policy and provide the adequate related training to help ensure IT systems are used for their intended purposes. The Board is responsible for establishing policies and procedures for all aspects of the Town's IT system to address crucial security areas, such as acceptable computer use, data backup, disaster recovery, breach notifications and policy violations. Furthermore, the Supervisor must ensure that the Town's server is located in a secure and safe location.

In 2007 the Board adopted an IT policy on acceptable computer use. However, the policy has not been updated since then and does not address data backup, disaster recovery, breach notifications or security awareness training. Furthermore, the Town's server is not located in a secure location. As a result, there is an increased risk that computerized data could be lost or compromised or that Town operations could be seriously disrupted.

Acceptable Use Policy

An effective process for safeguarding the Town's IT system includes an acceptable computer use policy, which defines the procedures for computer, Internet and email use and holds users accountable for properly using and protecting Town resources.

The Town has a computer use policy that addresses the terms and conditions for network, Internet and email use. However, the policy has not been updated since its creation in 2007 nor had the policy been distributed to Town officials and employees. When we told the Supervisor, she distributed the policy to all Town employees. However, without updating the computer use policy to reflect the ever changing IT developments, there is an increased risk that resources could be misused or that data could be lost or corrupted.

Data Backup

Sound business practices require that the Town's computer data be backed up (copied) on a daily basis so that it can be restored in the event of a loss. Back-up files should be kept in a secure off-site location to avoid loss from an event that could damage the Town's

IT system. In addition, it is important that back-up data files and restoration software be routinely tested for validity.

The Town uses an online service provider to back up its financial data to a remote location on a daily basis. However, the server and other computer data is not backed up nor have officials attempted to restore the data files to test the validity of the financial data backups. Town officials do not have formal policies or procedures addressing data backups, specifying which data files should be backed up or how often they should be backed up.

Without comprehensive data back-up procedures, which include periodically restoring backed-up data files, Town officials cannot be sure that all critical Town data is being backed up or that the backups performed can be used to successfully restore critical systems or data in the event of loss.

Disaster Recovery Plan

An effective internal control system for IT requires a formal disaster recovery plan (DRP) to prevent the potential loss of computer resources and to outline procedures for data recovery in the event of a disaster. A DRP, sometimes referred to as a business continuity plan or business process contingency plan, describes the precautions that must be taken to minimize the effects of a disaster and enable the organization to restore data and either maintain or quickly resume its mission critical functions. A DRP should provide for a back-up power source to allow an organization to continue to provide needed services not only during a disaster, but also through loss of power to the server.

The Board has not developed a DRP. Consequently, in the event of a disaster, Town personnel have no guidelines to minimize or prevent the loss of equipment and data, or how to implement data recovery and resume operations as efficiently as possible. The lack of a DRP could lead to loss of important financial data along with a serious interruption to Town operations, such as being able to process checks to pay vendors or employees.

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 (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.

The Board has not developed and adopted a breach notification policy because it was unaware of the Law. Without this policy, Town officials may not be able to notify individuals in a timely manner that their private information was acquired illegally.

Security Awareness Training

An important way to communicate IT security expectations to network users is by providing security awareness training to assist individuals with recognizing 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 IT security awareness training to ensure they understood the security measures designed to protect the Town's network. Officials were not aware that this training could help protect the Town's IT security. Employees' lack of training makes the Town's IT assets more vulnerable to loss and misuse.

Server Location

Physical security over computerized assets is an important component of overall computer and data security. The Supervisor must provide for the proper location of the server and implement procedures to ensure physical access is controlled so only authorized staff members have access to the server.

The Town's server is located in an area accessible to many employees and visitors, leaving the server only somewhat secure when certain employees are at their workstations. The Supervisor stated that the server was installed prior to her taking office and the location of the server was determined by the prior Supervisor. She also stated that when the employees' office is not open for regular business hours, the door is locked providing some added protection to the server. If access to the server is not controlled, the risk increases that unauthorized access to the network could be obtained and the server could be damaged.

Recommendations

The Board should:

1. Annually review and update the Town's comprehensive IT policy. This should include creating and adopting policies and procedures related to data backups, disaster recovery and breach notifications.
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 of the Town policy.

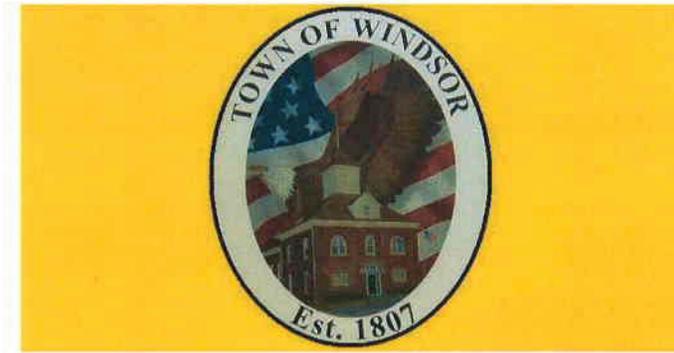
3. Ensure all network users receive IT security awareness training and that the training is updated whenever the IT policy is updated.

The Supervisor should:

4. Secure the Town's server so that only authorized individuals can gain access.

APPENDIX A
RESPONSE FROM LOCAL OFFICIALS

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



Supervisor Carolyn Price

Town of Windsor
124 Main Street
Windsor, New York 13865

Telephone number 607-655-2026
Facsimile 607-655-2027

May 10, 2017

Office of the State Comptroller
Division of Local Government
and School Accountability

The Town of Windsor (Town) agrees with the findings and recommendations in Report 2017M-44 (Report). The Town points out from the Report that an online service provider does backup its financial data to a remote location. Yes, at the time of the audit, Town officials had not tried to restore the data files to test the validity of the financial data backups. Since the audit, the Town has used financial data backup files to pay employees and found the process to work very well.

A written corrective action plan that addresses the findings and recommendations in the Report is in the process of being prepared and will be forwarded within ninety (90) days. The plan will include, but not be limited to, an updated information technology (IT) policy, documentation of Town personnel receiving the updated IT policy and IT security awareness training, and documentation of the removal of the server.

The Town appreciates Comptroller Office personnel doing the audit and giving the Town an opportunity to improve its IT operations. Through this audit, the Town is strengthening its controls to safeguard the Town's IT environment.

Sincerely,

Carolyn Price
Supervisor

William McIntyre
Deputy Supervisor

Timothy Bates
Councilman

Lesa Hawk-Shuler
Councilwoman

Gary Hupman
Councilman

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

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

- We interviewed Town officials to obtain an understanding of the Town's IT operations.
- We inquired as to policies and procedures related to acceptable computer use, data backups, disaster recovery plans, breach notifications, security awareness training and server locations.
- We examined four computers by running audit software and examined specific activities such as Internet use, Internet history and cookies.

We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
<http://www.osc.state.ny.us/localgov/>

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

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE

H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware,
Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE

Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie,
Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE

Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Albany, Clinton, Essex, Franklin,
Fulton, Hamilton, Montgomery, Rensselaer,
Saratoga, Schenectady, Warren, Washington Counties

HAUPPAUGE REGIONAL OFFICE

Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE

Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange,
Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE

Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

Serving: Cayuga, Chemung, Livingston, Monroe,
Ontario, Schuyler, Seneca, Steuben, Wayne, Yates Counties

SYRACUSE REGIONAL OFFICE

Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison,
Oneida, Onondaga, Oswego, St. Lawrence Counties

STATEWIDE AUDITS

Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313