



Town of Champion Information Technology

Report of Examination

Period Covered:

January 1, 2012 — December 31, 2013

2014M-130



Table of Contents

	Page
AUTHORITY LETTER	2
INTRODUCTION	3
Background	3
Objective	3
Scope and Methodology	4
Comments of Local Officials and Corrective Action	4
INFORMATION TECHNOLOGY	5
Administrative Rights	6
Data Backup	7
Breach Notification	7
Disaster Recovery	7
Recommendations	8
APPENDIX A Response From Local Officials	9
APPENDIX B Audit Methodology and Standards	13
APPENDIX C How to Obtain Additional Copies of the Report	14
APPENDIX D Local Regional Office Listing	15

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

July 2014

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 Champion, 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 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 Champion (Town) is located in Jefferson County (County) and has a population of approximately 4,500. The Town is governed by an elected five-member Town Board (Board) which comprises the Town Supervisor (Supervisor) and four Board members. The Board is responsible for the general management and control of the Town's assets, including computerized data. The Supervisor serves as chief executive officer. The Town has an unpaid volunteer information technology (IT) consultant who maintains the Town's computer network.

The elected Town Clerk is also the Tax Collector and is responsible for collecting and depositing Town and County real property taxes, water and sewer rents, and other fees (dog licenses, hunting and fishing licenses, marriage licenses, transfer site fees and zoning/land use permits). The Town Clerk/Tax Collector accepts payment of taxes, water and sewer rents, and other fees by credit card at the Town's office and online through its website.¹ In 2013, the Town collected more than \$28,000 in these fees by credit card at the Town's office and approximately \$7,800 online. The Town Clerk remotely deposits² checks for payment of taxes and fees and assists the Town Supervisor by remotely depositing other checks received by the Town. The 2013 tax warrant for Town and County taxes was approximately \$2.8 million; other non-property tax revenues collected totaled approximately \$2.1 million in 2013.

The Town's budgeted expenditures for the 2014 fiscal year were approximately \$2.5 million. These expenditures are primarily funded with revenues from real property taxes, sales tax, water and sewer rents, and State aid.

Objective

The objective of our audit was to review the Town's internal controls over its computer network. Our audit addressed the following related question:

- Are internal controls over the Town's computer network appropriately designed and operating effectively to ensure that the Town Clerk/Tax Collector's electronic transaction processes are adequately safeguarded?

¹ Town residents can also pay taxes online through the Jefferson County Real Property Tax website.

² Remotely depositing refers to a process where the Town has a scanner that is capable of reading the magnetic ink/information on checks and automatically depositing the money into the Town's bank account.

**Scope and
Methodology**

We examined internal controls over the Town’s computer network for the period January 1, 2012 through December 31, 2013. We extended our scope period to perform certain tests of the Town’s network security controls through February 26, 2014. Our audit disclosed additional areas in need of improvement concerning IT controls. 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 in a separate letter so that they could 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 is 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 findings and recommendations and indicated that they have already implemented their corrective action plan.

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 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 its operations. It is used for accessing the Internet, communicating by email, processing and storing data, maintaining water and sewer billing records, maintaining tax and other Town Clerk/Tax Collector records, accepting credit card payments, remotely depositing checks and reporting to State and Federal agencies. Therefore, it is imperative that Town officials ensure that computerized data is properly safeguarded. Accordingly, the Board is responsible for establishing policies and procedures to help protect the Town's computer equipment and data against the risk of loss, misuse or improper disclosure of sensitive data. This includes ensuring that individuals have only the access rights necessary to perform their job duties. The Board also should develop a comprehensive IT disaster recovery plan — to provide guidance on the recovery of data in the event of a disaster — and a breach notification policy to provide guidance in the event that private data is released to unauthorized individuals.

The IT consultant told us that there are no physical email or web servers located at the Town's offices and that there is only one Internet connection for all computers³ located at the Town's offices. The computers are linked through the Internet connection, and there are two wireless routers.⁴ The Town Clerk has three desktop computers in her office that are used for various purposes. One computer is used for recording cash receipts and has an attached credit card scanner. A second computer is used for email, Internet use, online banking (statement viewing and transfers), as well as the water and sewer billing systems. The Clerk uses the third computer solely for the remote deposit of checks. She also has a laptop computer which she uses for downloading meter readings for water and sewer billings.

Due to the Town Clerk's reliance on computer technology for cash collection and banking transactions, it is imperative that Town officials ensure that the computerized data is properly safeguarded. The Board needs to improve internal controls to effectively protect the Town's computer system and data. Specifically, the Board needs to restrict administrative rights to those who need them to perform their jobs. In addition, the Town needs to store copies of back-up data in a secure

³ There are total of eight desktop computers and three laptops computers that Town employees use to access to the Town's network. This includes the computers used by the Town's Justice Court.

⁴ One wireless router is located in the Town Clerk's office, and one is located in the Town's Justice Court.

offsite location, and the Board needs to develop a disaster recovery plan. As a result of these weaknesses, there is an increased risk of loss of critical data and interruptions to Town operations. In addition, the Board should periodically review the Town's breach notification policy and ensure that employees are adequately prepared to notify affected individuals in the event that their private information is compromised.

Administrative Rights

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.

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, creating/modifying/deleting user accounts, gaining unauthorized access to all file shares or data resources, extracting password hashes⁵ for all users, and turning on or off network services.

Also, when a user authenticates as a member of the Administrators group, the user's profile, including any programs that the user initiates, will run with the full access rights and permissions of an administrator. A user with administrative rights can make system-wide changes, including installing programs of their own choosing and manipulating settings configured for security purposes. As a result, if malware is able to install itself on the system, it would run at a higher privilege under a user account with administrator rights, resulting in a higher risk of data loss or compromise.

According to the Town's IT consultant, all users have administrator rights to their computers. We verified this on the three computers⁶ that we manually examined during our onsite testing.

To protect the Town's network and data it holds, users should not use an administrative account for normal tasks. If administrative rights are needed for certain duties of a user's job, a separate account with

⁵ Numerical representation of a password

⁶ The three computers included the computer used to process remote bank deposits, the computer used to process real property tax payments, and the Town Clerk's computer.

administrator rights should be created and used only when needed. The remediation of this serious internal control weakness should not require an exhaustive effort or additional costs since the Town already has the necessary infrastructure in place to make the required changes.

Data Backup

A strong system of internal controls includes a system to back up (create a copy of) computer-processed data. Good business practices require Town officials to run daily backups, keep the backup data as current as possible, and store the data at an environmentally and physically secure offsite location for retrieval in case of an emergency. They should also periodically test backups to ensure that the data could actually be restored in the event of a data loss.

Town officials have not adopted comprehensive data backup policies and procedures for computer-processed data. The Clerk told us she backs up electronic data for the Town Clerk receipt, Tax Collector receipt, and water and sewer billing software. However, the Clerk backs up the data to the machine that she is currently working on and not to an offsite location or a removable hard drive. She does not back up any of her other computer files. As a result, the Town is at risk of losing most, if not all, of the computerized data processed by the Clerk if the system becomes compromised and a backup is not available to restore it to normal operation.

Breach Notification

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. 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.

During our fieldwork, Town officials informed us that the Board had not adopted a breach notification policy. However, after our exit discussion, officials located a policy that had been adopted by the Board in April 2006. Because Town officials and employees were not aware of the policy, they may not have been prepared to notify affected individuals in the event that private information had been compromised.

Disaster Recovery Plan

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 to prevent loss of computer equipment and data, including the procedures for recovery in the event of an actual loss, is crucial to an organization. The plan needs to address the roles of key individuals and include 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. Disaster recovery planning also involves an analysis of continuity needs and threats to business processes and may include significant focus on disaster prevention.

The Board has not established a formal 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 data recovery and resume operations as efficiently as possible. The failure to establish a disaster recovery plan could result in the loss or damage of essential information which may not be recoverable.

Recommendations

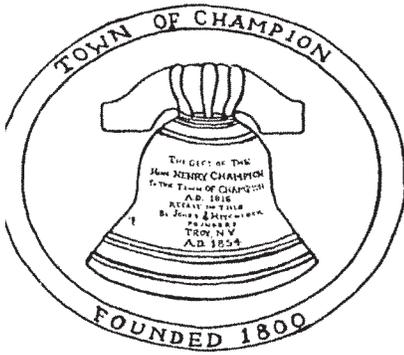
1. Town officials should restrict administrator rights to computers. If administrator rights are needed for certain duties of a user's job, Town officials should create a separate account with administrative rights and use it only when needed.
2. Town officials should ensure that all of the Town's data is backed up to a secure off-site location, and that procedures are developed to periodically test and restore back-up data to ensure that it is complete, accurate and useable.
3. The Board should periodically review the breach notification policy.
4. The Board should develop a formal disaster recovery plan identifying potential risks and detailing the responses to be taken. This plan should be distributed to all responsible parties, periodically tested and updated as needed.

APPENDIX A

RESPONSE FROM LOCAL OFFICIALS

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

The Town's response letter refers to an attachment of the Town's Information Technology Disaster Recovery Plan. Because the Town's response letter provides sufficient detail of its actions, we did not include the attachment in Appendix A.



TOWN OF CHAMPION
10 NORTH BROAD STREET
CARTHAGE, NEW YORK 13619

Tel: 315-493-3240
Fax: 315-493-2900
TDD: 1-800-662-1220
www.racog.org

July 8, 2014



Office of the State Comptroller
110 State St
Albany, NY 12236

Re: Town of Champion
2014M-130
Information Technology

Dear :

The Town of Champion Town Board has reviewed the draft Report of Examination conducted for the period January 1, 2012 – December 31, 2013.

The Town Board agrees with the recommendations set forth in the draft report. For each recommendation included in the audit report, the following is our corrective actions taken or proposed.

Thank you for the time and effort your staff put into this audit. The exit discussion was thorough and well articulated.

Respectfully,

Terry E. Buckley 
Town Supervisor

Enc.

This institution is an equal opportunity provider, and employer. To file a complaint of discrimination, write: USDA, Director, Office of Civil Rights, 1400 Independence Avenue S.W., S.W., Washington, D.C. 20250-9410, or call (800) 795-3272 (voice) or (202) 720-6382 (TDD).

Audit Response & Correction Action Plan

Audit Recommendation: Town officials should restrict administrator rights to computers; if administrator rights are needed for certain duties of a user’s job, Town officials should create separate accounts with administrative rights and use it only when needed.

Implementation Plan of Action: Separate accounts shall be set up with administrative rights for use as necessary.

Implementation Date: Separate administrative accounts have been established.

Person Responsible for Implementation: Town of Champion Town Board directed the technology consultant to implement the action.

.....

Audit Recommendation: Town officials should ensure that all of the Town’s data is backed up to a secure off-site location, and that procedures are developed to periodically test and restore back-up data to ensure that it is complete, accurate, and useable.

Implementation Plan of Action: The Board contracted for the daily electronic transfer of encrypted data via the Internet to a remote location for safekeeping to insure that data and related applications are secure and readily available in the event of computer failure or disaster.

Implementation Date: The daily electronic transfer of data has commenced and is on-going.

Person Responsible for Implementation: Town of Champion Town Board and the Town Clerk.

.....

This institution is an equal opportunity provider, and employer. To file a complaint of discrimination, write: USDA, Director, Office of Civil Rights, 1400 Independence Avenue S.W., S.W., Washington, D.C. 20250-9410, or call (800) 795-3272 (voice) or (202) 720-6382 (TDD).

Audit Recommendation: The Board should periodically review the breach notification policy.

Implementation Plan of Action: The Board will periodically review the breach notification policy in conjunction with other policy reviews.

Implementation Date: The policy was reviewed on July 7, 2014. No changes were made.

Person Responsible for Implementation: Town of Champion Town Board implemented the action.

.....

Audit Recommendation: The Board should develop a formal disaster recovery plan identifying potential risks and detailing responses to be taken. This plan should be distributed to all responsible parties, periodically tested and updated as needed.

Implementation Plan of Action: The Board developed an information technology disaster recovery plan that identifies potential risk scenarios and details the response by department.

Implementation Date: The policy was reviewed and adopted on July 7, 2014. A copy of the Town of Champion Information Technology Disaster Recovery Plan is attached.

Person Responsible for Implementation: Town of Champion Town Board and Town Clerk implemented the action.


Terry L. Buckley
Town Supervisor

7-7-14
Date

This institution is an equal opportunity provider, and employer. To file a complaint of discrimination, write: USDA, Director, Office of Civil Rights, 1400 Independence Avenue S.W., S.W., Washington, D.C. 20250-9410, or call (800) 795-3272 (voice) or (202) 720-6382 (TDD).

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

During the initial assessment, we interviewed appropriate Town officials, performed limited tests of transactions, 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. Based on that evaluation, we determined that controls appeared to be adequate and limited risk existed in most of the financial areas we reviewed. We then decided on the reported objective and scope by selecting for audit the area most at risk: internal controls over the Town's network. To accomplish the objective of this audit and obtain valid audit evidence, our procedures included the following:

- We interviewed the Town Supervisor, Town Clerk and the volunteer IT consultant to obtain an understanding of the Town's computer network.
- We interviewed and observed the Town Clerk to obtain an understanding of procedures for over the counter and online credit transactions.
- We reviewed the Town Clerk and Tax Collector bank statements for any credit card withdrawals.
- We interviewed and observed the Town Clerk to obtain an understanding of procedures for remotely depositing checks.
- We examined the Town Clerk's three computers by running audit software and examining temporary internet files, cookies and internet histories.

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
Nathalie 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-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