DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2020M-126

Town of Wolcott

Information Technology

JUNE 2021

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Town of Wolcott

Audit Objective

Determine whether the Town Board (Board) ensured the Town of Wolcott's (Town) information technology (IT) assets were adequately safeguarded.

Key Findings

The Board did not ensure that IT assets were adequately safeguarded. The Board did not:

- Adopt any IT policies or a disaster recovery plan.
- Provide users with cybersecurity awareness training.
- Ensure the financial software, Town Clerk's software and Justice Court software had the necessary controls to maintain data integrity.

Sensitive IT control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt IT policies and a disaster recovery plan.
- Provide cybersecurity awareness training.
- Consider upgrading department software or implement compensating controls for software deficiencies.

Town officials generally agreed with our recommendations and indicated they plan to initiate corrective action.

Background

The Town is located in Wayne County and includes the Villages of Wolcott and Red Creek.

The Town is governed by an elected Board composed of the Supervisor and four Board members. The Board is responsible for the general management of Town operations.

The Supervisor is the chief executive officer and is responsible for the Town's day-to-day activities, including managing IT assets. The Town relies on the Supervisor's clerk for the overall management of its IT infrastructure and engages a vendor for IT support and services as needed.

Quick Facts

	Town Hall
Computers	7
Officials and Employees	22

Audit Period

January 1, 2016 – November 19, 2019

Information Technology

The Town uses information technology (IT) systems to initiate, process, record and report transactions. The Town also relies on its IT systems for accessing the Internet, emailing and maintaining financial information. The Town's software contains personal, private and sensitive information (PPSI).[1] The Town's IT systems and data are valuable resources which if compromised could require extensive effort and resources to evaluate and repair.

What IT Security Policies Should the Board Adopt to Safeguard Data?

Town officials are responsible for developing comprehensive written policies and procedures to properly protect PPSI from unauthorized access.[2] New York State Technology Law[3] requires local governments to adopt a breach notification policy that details actions to be taken to notify affected individuals if PPSI is compromised. The board should also adopt an acceptable use policy, which defines the procedures for computer, internet and email use and holds users accountable for properly using and protecting town resources. To ensure the highest level of security over town data, the board should also adopt policies for security management including policies for individual user accounts, online banking, use and access to PPSI and backups. All IT policies should be periodically reviewed and updated to reflect changes in technology and the computing environment.

Town officials are responsible for developing comprehensive written policies and procedures to properly protect PPSI from unauthorized access.

The Board Did Not Adopt IT Policies

The Board did not adopt any IT policies, including those related to breach notification, acceptable use, user accounts, passwords, online banking, use and access to PPSI, backups, audit logs and change reports. Town officials were not aware of the requirement and need for IT policies.

While policies alone will not guarantee the safety of IT assets and data, a lack of appropriate policies significantly increases the risk that the Town could lose important data, suffer a serious interruption in operations and unauthorized individuals could access computerized data to copy, manipulate or delete sensitive information. Without formal policies that specify appropriate computer use and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities. Additionally, officials may not be able to notify individuals in a timely manner in the event that their private information was accessed.

[1] PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, customers, third parties or citizens of New York in general. PPSI could include: Social Security number, driver's license number or non-driver identification card number, account number, or access code/password that permits access to an individual's financial account.

[2] For guidance on recommended IT policies refer to our Local Government Management Guide – Information Technology Governance at: https://www.osc.state.ny.us/files/local-government/publications/pdf/itgovernance.pdf

[3] New York State Technology Law Section 208

Why Should the Board Provide Security Awareness Training?

Computer users need to be aware of security risks and be trained in practices that reduce internal and external threats to IT systems and data. While IT policies provide guidance for computer users, cybersecurity training helps them understand their roles and responsibilities and provides them with the necessary skills to perform them. Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything needed to perform their jobs. IT security awareness should reinforce IT policies and can focus on security in general or a narrow aspect of security (e.g., the dangers of opening an unknown email or attachment or downloading files from the Internet).

The Board Did Not Provide Security Awareness Training

The Board did not provide users with cybersecurity awareness training to help ensure they understand security measures to protect IT assets. As a result, users may not be aware of risks and inadvertently expose the Town's IT assets to cybersecurity attacks, loss and misuse.

Why Should Town Officials Provide Unique Login Credentials For Each User?

Effective access controls require that user accounts be linked to specific individuals to help prevent and detect unauthorized or inappropriate activity and to provide accountability for all transactions. Users should not be allowed to share accounts. Further, software access rights should be assigned based on each user's job responsibilities.

Town Officials Did Not Provide Unique Login Credentials for Each User

The Town Clerk and the deputy clerk shared a user account to access the computer and software used in the Town Clerk's office. The clerks believed it was more convenient to share a username and were unaware that this was not an ideal practice. Without unique login credentials to link user accounts to specific individuals with properly authorized access rights, there is an increased risk of unauthorized or inappropriate activity. Further, accountability is diminished and system activity may not be traceable to a single user.

The Town Clerk and the deputy clerk shared a user account to access the computer and software used in the Town Clerk's Office.

How Should Officials Manage Application User Accounts?

Once information is entered into the software, its integrity should be maintained through controls that limit access and changes to data to ensure that transactions are not altered. It is essential to ensure that deletions and adjustments cannot be made without authorization and that there is a process in place to review data entered into and changed in the system. A control weakness allowing deletions or changes to data could allow a user to conceal a theft by issuing a receipt to a customer for the amount received and then deleting that receipt or issuing an unauthorized check and subsequently deleting the check or changing the vendor name in the software disbursement record. If software-generated receipt numbers can be altered, the departments should use and retain copies of pre-numbered manual receipts. The receipt sequence should be periodically reviewed and any missing or duplicate receipt numbers investigated.

Certain Software Did Not Require Authorization for Adjustments, Deletions or Changes to Data

We found that the software used to maintain the Town's financial information and the software used by the Town Clerk's office and Justice Court did not have the necessary controls to maintain data integrity. All of these software applications allowed changes and deletions to the data without approval; including data and receipt number changes, voided transactions, deletions or adjustments to receipt amounts or vendor names and amounts of disbursements. Altering, adding or deleting data increases the risk of inappropriate disbursements or that funds could be received but not deposited or reported.

Although the Town Clerk's office issues manual receipts before receipts are entered into the software, the receipts are not pre-numbered. The Justice Court issues pre-numbered duplicate manual receipts and the court clerk then enters the pre-numbered receipt number as the receipt number in the software. However, the Justices do not review the physical duplicate receipt sequence. In addition, there are no controls preventing an electronic receipt from being issued without a manual receipt having been issued or from an electronic receipt number being used multiple times. This control weakness would be resolved by upgrading to the newer software version. However, officials were not aware that there was a more secure version of the Justice Court software available. The Supervisor's clerk told us that she was aware of the financial software's control deficiencies. However, she is familiar with the software used and does not want to maintain manual records.

Why Should Audit Logs Be Regularly Reviewed for Questionable Activity?

An audit log is an automated mechanism for establishing individual accountability, reconstructing events and monitoring problems. Audit logs maintain a record of activity that includes the identity of each person who has accessed the software, the time and date of the access and what activity occurred. Town officials should periodically review these logs to monitor the activity of persons who access financial records and identify problems that may have occurred.

Audit Logs Were Not Reviewed or Were Not Available

When control deficiencies exist, mitigating controls should be implemented. An effective monitoring tool is the regular review of user access and activities logged within the software. However, a log was not available in the version of the software used by the Justice Court. Additionally, logs or reports of changes were not reviewed for the financial software or software used by the Town Clerk's office.

Town officials did not develop, and the Board did not adopt, a disaster recovery plan…

Why Should the Town Have a Disaster Recovery Plan?

A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services in the event of a disaster. Such disasters may include any sudden, catastrophic event (e.g., fire, flood, computer virus or inadvertent employee action) that compromises the availability or integrity of the IT system and data. Typically, a disaster recovery plan involves an analysis of business processes and continuity needs, a focus on disaster prevention, the roles of key individuals and precautions to maintain or quickly resume operations. Additionally, the disaster recovery plan should include procedures for routine backup of applications and data, secure offsite storage of backup media and periodic testing of the backups to ensure they function as expected. The plan should be distributed to all responsible parties, periodically tested and updated as needed.

The Town Does Not Have a Disaster Recovery Plan

Town officials did not develop, and the Board did not adopt, a disaster recovery plan including procedures for the routine backup of application and data, secure storage of backup media, and periodic testing of the backups to ensure they can be properly restored in the event of loss.

Although officials told us that backups were performed, officials did not test the backups for the financial software or Town Clerk's software to ensure they were effective and could be relied on for service continuity. Additionally, the clerk put the financial software backup on a storage device that was kept in a location near the laptop with the financial software. As a result, the original data and backup could both be destroyed in a physical disaster.

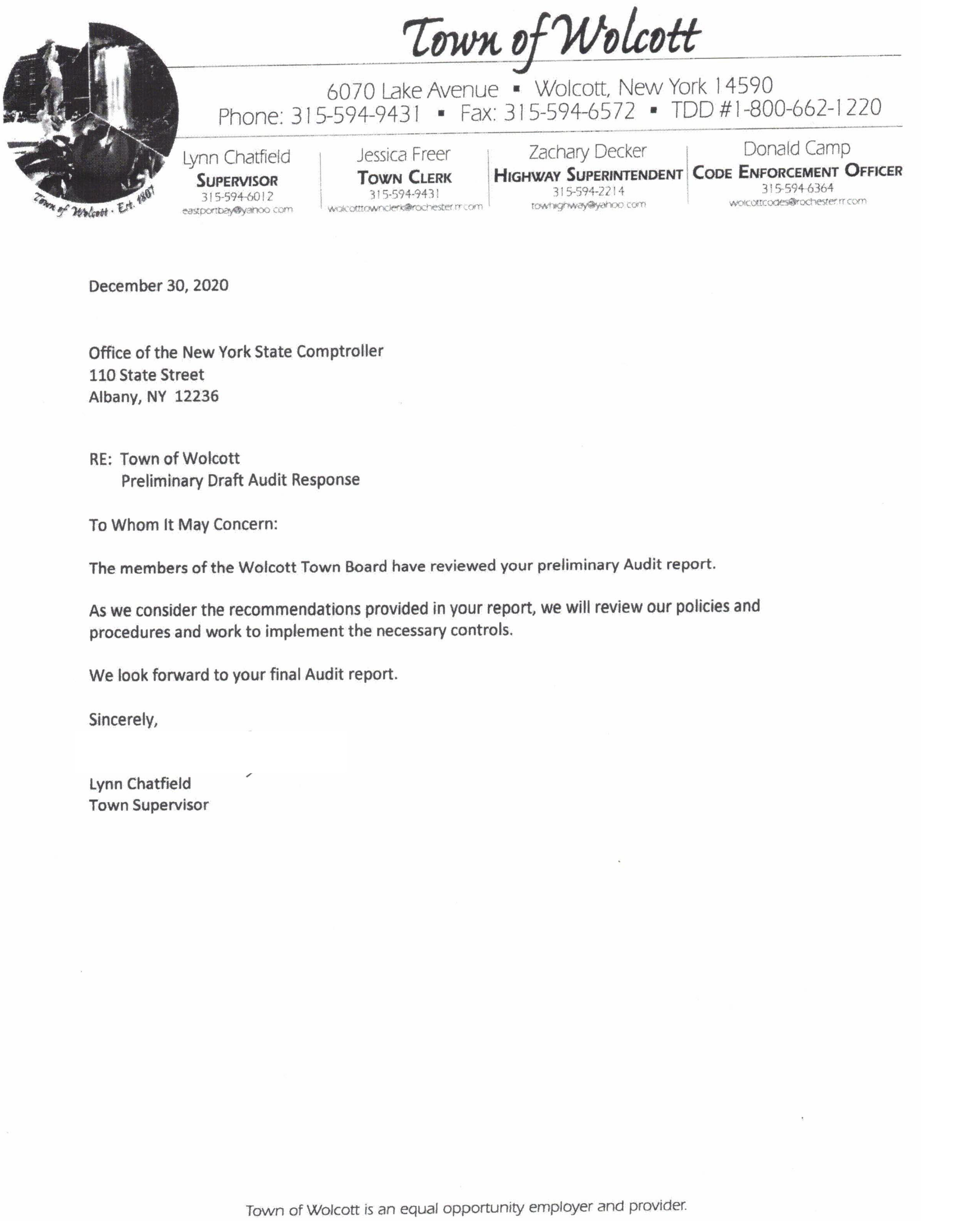
Without a comprehensive disaster recovery plan and procedures for data backup and secure storage, the Town is at increased risk of losing critical information and incurring costly interruption of operations, such as not being able to process checks to pay vendors.

What Do We Recommend?

The Board should:

1. Adopt written IT policies including those to address acceptable use, breach notification, user access, password security, PPSI, backups and online banking.
2. Provide IT security awareness training to personnel who use IT resources.
3. Ensure that all users have their own unique username for the computer and software.
4. Consider upgrading department software or implement compensating controls for software deficiencies.
5. Develop a comprehensive disaster recovery plan and procedures for backing up data and applications. Ensure that appropriate personnel know these processes and periodically test the Town's disaster recovery plan and backups to ensure they will function as expected.

Appendix A: Response From Town Officials



Town of Wolcott

6070 Lake Avenue ▪ Wolcott, New York 14590
Phone: 315-594-9431 ▪ Fax: 315-594-6572 ▪ TDD #1-800-662-1220

Lynn Chatfield	Jessica Freer	Zachary Decker	Donald Camp
Supervisor	Town Clerk	Highway Superintendent	Code Enforcement Officer
315-594-6012	315-594-9431	315-594-2214	315-594-6364
eastportbay@yahoo.com	wolcotttownclerk@rochester.rr.com	townhighway@yahoo.com	wolcottcodes@rochester.rr.com

December 30, 2020

Office of the New York State Comptroller
110 State Street
Albany, NY 12236

RE: Town of Wolcott
Preliminary Draft Audit Response

To Whom It May Concern:

The members of the Wolcott Town Board have reviewed your preliminary Audit report.

As we consider the recommendations provided in your report, we will review our policies and procedures and work to implement the necessary controls.

We look forward to your final Audit report.

Sincerely,

Lynn Chatfield
Town Supervisor

Town of Wolcott is an equal opportunity employer and provider.

Appendix B: Audit Methodology and Standards

We conducted this audit 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. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We interviewed Town officials and employees and reviewed Board minutes and policies to gain an understanding of IT controls and the IT environment.
- We observed as Town officials and employees showed us how they access computers and software and certain available features and reporting options.

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 this performance audit in accordance with GAGAS (generally accepted government auditing standards). 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.

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.

A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and provided 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 the CAP available for public review in the Clerk's office.

Appendix C: Resources and Services

Regional Office Directory
https://www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
https://www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
https://www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
https://www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
https://www.osc.state.ny.us/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/local-government

Local Government and School Accountability Help Line: (866) 321-8503

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

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

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller