New York State Comptroller
THOMAS P. DiNAPOLI

Town of Plattekill

Information Technology

2025M-132 | April 2026

Division of Local Government and School Accountability

Contents

Audit Results

Town of Plattekill

Audit Objective	Audit Period
Did the Town of Plattekill (Town) Town Board (Board) and Town Supervisor (Supervisor) adequately manage the Town's network user accounts and develop adequate controls to safeguard information technology (IT) resources?	January 1, 2023 – August 12, 2024 We extended our audit period through October 8, 2024 for observations of certain IT controls communicated confidentially to Town officials.

Understanding the Audit Area

Town officials must manage network user accounts and develop adequate controls to minimize the risk of unauthorized use, access and loss. Network user accounts are potential entry points for attackers because, if compromised, they could be used to inappropriately access and view personal, private, sensitive information (PPSI)[1] on the network, make unauthorized changes to official town records or deny legitimate access to network resources. Adequate controls, like security awareness training, can help reduce the risks of attack by preparing personnel to respond in a practiced and cohesive way. These measures are essential components of a robust cybersecurity control environment, which is vital for effective and responsible governance, and helps safeguard resources against financial loss and ensure critical functions continue.

The Town paid a third-party IT service provider $5,928 during the audit period for IT services upon request, including IT support, network setup and maintenance, and other IT-related services, for the Town's 28 enabled network user accounts.

Audit Summary

The Board and Supervisor did not adequately manage network user accounts or develop adequate controls to safeguard IT resources. As a result, the Board and Supervisor cannot be assured that Town IT systems are secured and protected against unauthorized use, access and loss, and there is an

1 PPSI is any information to which unauthorized access, disclosure, modification, destruction or use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers, third parties or other individuals or entities.

increased risk that officials could lose important data and suffer a serious interruption in operations. Weaknesses in policies, oversight and other internal controls increase the risk that network user accounts and hardware or software systems may be lost, damaged or compromised.

We determined the Board and Supervisor did not:

- Disable 14 unneeded network user accounts that were assigned to former Town employees with separation dates between November 17, 2016 and December 31, 2023.
- Develop and adopt a breach notification policy as required by New York State Technology Law (Technology Law) Section 208.
- Develop and adopt an IT contingency plan for unexpected IT disruptions or disasters.
- Require all employees to take IT security awareness training.
- Enter into a written contract or service level agreement (SLA) with the Town's IT service provider.

Sensitive IT control weaknesses were communicated confidentially to officials.

The report includes six recommendations that, if implemented, will improve the Town's IT practices over network user accounts and safeguarding IT resources. Town officials generally agreed with our recommendations, and their response is included in Appendix B.

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the Office of the New York State Comptroller's (OSC) authority as set forth in Article 3 of the New York State General Municipal Law (GML). Our methodology and standards are included in Appendix C.

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 provided to our office within 90 days, pursuant to Section 35 of GML. 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.

Information Technology: Findings and Recommendations

Network user accounts provide access to network resources and data needed by employees to complete job duties and other work-related responsibilities. Town officials should ensure network user accounts are adequately managed by developing written procedures for granting, changing and revoking access to the network, including disabling former employees' accounts the day they separate from the town.

A town board must adopt a breach notification policy that details actions to be taken to notify affected individuals if private information is compromised and should adopt a written IT contingency plan to help minimize the risk of data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster.

Town officials should also provide IT security awareness training to ensure employees understand IT security measures, their responsibilities, and how to safeguard data from potential misuse or loss. In addition, a town board should enter into a formal written contract with the IT service provider that sufficiently defines the contractual relationship and responsibilities between both parties.

More details on the criteria used in this report, as well as resources/publications we make available to officials to help improve operations (Figure 1), are included in Appendix A.

Finding 1 – The Board and Supervisor did not ensure unneeded network user accounts were disabled.

The Board and Supervisor did not develop written policies and procedures for granting, changing, and disabling unneeded network user accounts, or routinely evaluating and disabling any unneeded network user accounts in a timely manner. We reviewed all 28 enabled network user accounts and identified 14 user accounts (50 percent) that were unneeded and should have been disabled. These accounts were assigned to former Town employees with separation dates between November 17, 2016 and December 31, 2023. Further review showed that 11 of the 14 user accounts (79 percent) were still being used after the employees separated from the Town. For example, a network user account assigned to an employee who separated from the Town on July 2, 2020 was last logged into on July 31, 2024, just over four years later. The confidential secretary to the Supervisor (confidential secretary) stated the user accounts were not disabled because they did not contact the IT service provider to transfer information saved on the computers from previous employees. Current Town employees are using the former employees' accounts to access information when they need to.

The Supervisor stated that the unneeded accounts were not deleted due to his lack of awareness of IT best practices. In addition, the Supervisor mentioned that he had not taken any training specifically related to IT that would have assisted him with this awareness. Furthermore, he stated that he did not have sufficient time to develop IT policies and procedures while maintaining his other supervisor duties.

When not adequately managed, unneeded network user accounts may not be detected and disabled in a timely manner. When unneeded network user accounts remain enabled, they are potential entry points for attackers because, if compromised, they could be used to inappropriately access the network

and view PPSI accessible through that account's access, make unauthorized changes to Town records, deny legitimate access to electronic information, or gain access to or control over other IT functions. Additionally, if users share accounts, accountability is diminished and activity in the system may not be able to be traced back to a single user.

Recommendations

1. The Board should develop written policies and procedures for granting, changing, and disabling unneeded network user accounts and ensure they are distributed to all applicable staff.
2. The Supervisor should ensure network user accounts are routinely evaluated and disable any unneeded network user accounts in a timely manner.

Finding 2 – The Board did not develop adequate controls to safeguard IT resources.

Specifically, the Board did not:

- Develop and adopt a breach notification policy as required by Technology Law Section 208. The Supervisor said he was not aware that the Town was required to have a breach notification policy. Without a breach notification policy, if a network user account is compromised, it could result in the compromise of private information, or a reasonable belief this information was compromised, and officials and employees may not understand or be prepared to fulfill their legal obligation to notify affected individuals.
- Develop and adopt an IT contingency plan. The Supervisor said he was not aware that the Town should have an IT contingency plan because he had limited time to gain a better understanding of IT requirements while maintaining his other supervisory duties. Without an IT contingency plan, officials cannot be assured that in the event of an unplanned IT disruption or disaster, they would be able to restore critical IT systems, applications or data in a timely manner. Depending on the severity of an incident, officials may need to expend significant time and financial resources to resume Town operations.
- Provide periodic IT security awareness training for employees who have access to the town's computer network. We determined that 14 of the 77 Town employees use computers that have access to the Town's computer network and 11 of the 14 employees (79 percent) did not receive IT security awareness training. The Supervisor said he was not aware that IT security awareness training should be required for Town officers and employees with access to the Town's network and potential access to PPSI. Failure to provide IT security awareness training increases the risk

that users will not understand their responsibilities, putting their network user accounts and the Town's data and IT network at greater risk for unauthorized access, misuse or abuse.

- Enter into a written contract or SLA with the Town's third-party IT service provider. The Town paid the IT service provider $5,928 for IT services for the audit period. The Supervisor said he was not aware of the importance of having a contract or SLA with the IT service provider but acknowledged the benefits that they would provide for the Town. The confidential secretary stated that the Town had an SLA with the IT service provider more than 10 years ago when services started, but the confidential secretary and IT service provider could not provide us with the SLA. Without a comprehensive written contract or SLA, officials could not ensure the Town was receiving the services which it paid for and should have received. In addition, insufficient, nonexistent or vague agreements can contribute to confusion over who has responsibility for various aspects of the IT environment, such as managing network user accounts, which puts data and the IT network at greater risk for unauthorized access, misuse or loss.

Recommendations

The Board should:

3. Develop and adopt a breach notification policy as required by Technology Law Section 208.
4. Develop and adopt a comprehensive written IT contingency plan, update the plan as needed, and distribute it to all responsible parties.
5. Ensure IT security awareness training is periodically provided to all users of the Town's IT network.
6. Enter into a written contract or SLA with the IT service provider that sufficiently defines the roles and responsibilities of each party, specifies IT service pricing and includes all services to be provided.

Appendix A: Profile, Criteria and Resources

Profile

The Town, located in Ulster County, is governed by an elected Board composed of the Supervisor and four Board members. The Board is responsible for the general oversight of Town operations, which includes adopting policies to help safeguard the Town's IT network and assets, such as network user accounts and servers. The Supervisor is responsible for ensuring IT policies, guidelines and procedures are implemented effectively. The Town's third-party IT service provider performed IT services upon request for the Town's 28 enabled network user accounts and 31 network computer accounts (servers, desktops and laptops). The confidential secretary acts as the primary liaison with the Town's IT service provider, including coordinating service requests.

Criteria – Information Technology

The town board should adopt policies that describe the tools and procedures used to help protect IT systems, including data and networked applications, and help define the expectations for appropriate user behavior and explain the consequences of policy violations. Although no single practice or policy on its own can adequately safeguard an IT network from cybersecurity risks, there are several practices that, if properly enacted and monitored, decrease the chances of a successful attack.

Town officials should ensure unneeded network user accounts are disabled in a timely manner by developing and enforcing written procedures for disabling user accounts and distribute the procedures to applicable staff. Additionally, town officials should maintain a list of authorized network user accounts and routinely review enabled network user accounts to ensure they are still necessary or adjust access rights accordingly.

Technology Law Section 208 requires municipalities and other local agencies to have a breach notification policy or local law. This policy details actions to be taken to notify affected individuals if private information is compromised.

The town board should develop and adopt a comprehensive written IT contingency plan to help minimize the risk of data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster. A disruptive event could include a power outage, software failure caused by a virus or malicious software, equipment destruction, inadvertent employee action or a natural disaster (e.g., a flood or fire), that compromises the availability or integrity of town services, including the IT system and data. IT contingency planning involves analyzing business processes and continuity needs, focusing on sustaining critical functions and identifying roles of key individuals and necessary precautions needed to maintain or quickly resume operations. The plan should be periodically tested and updated to ensure officials understand their roles and responsibilities in a disaster situation or other unexpected IT disruption and to address changes in security requirements. In addition, a plan should include data backup procedures and periodic backup testing to ensure backups will function as intended.

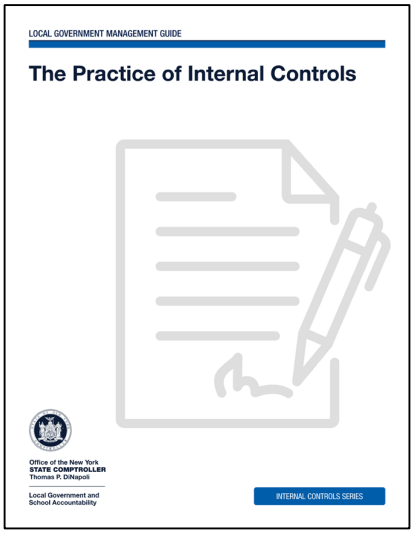
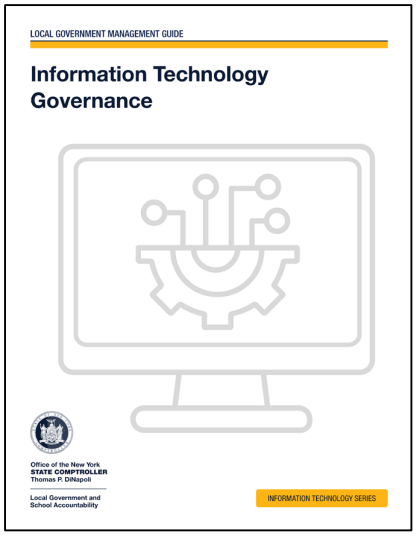
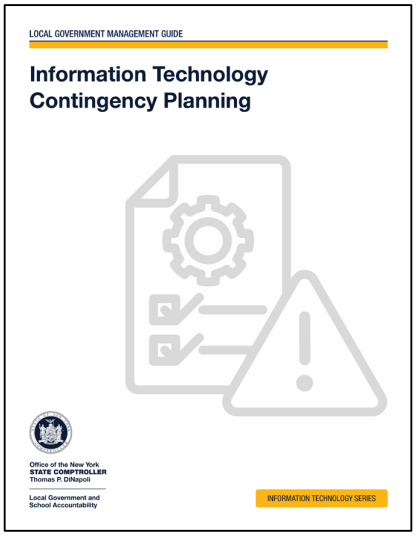
To minimize the risk of unauthorized access and misuse or loss of data and PPSI, town officials should provide periodic IT security awareness training to all employees who have access to the network. Training should keep town officials and employees current on evolving security threats and the policies and procedures that should be in place to reduce risk. The training should include town policies and procedures, and the proper rules for using the Internet, IT network and data.

The town board should enter into a written agreement between the town and the IT service provider that specifies the level of service to be provided by the IT service provider. The agreement should clearly state the needs and expectations of the town and any legal requirements relating to the confidentiality and protection of PPSI.

Additional IT Resources

Figure 1: OSC Publications

OSC *Local Government Management Guides* and other informational resources are available on our website to help officials understand and perform their responsibilities and implement effective internal controls.

The Practice of Internal Controls	*Information Technology Governance*	*Information Technology Contingency Planning*
		
https://www.osc.ny.gov/files/local-government/publications/pdf/the-practice-of-internal-controls.pdf	https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf	https://www.osc.ny.gov/files/local-government/publications/pdf/itcontingencyplanning.pdf

In addition, our website can be used to search for audits, resources, publications and training for officials: https://www.osc.ny.gov/local-government.

Appendix B: Response From Town Officials

TOWN OF PLATTEKILL
SUPERVISOR MICHAEL LEMBO

March 26, 2026

James L. Laitaner, Chief of Municipal Audits
Office of the State Comptroller, Newburgh Regional Office

Re: Response to Audit Findings Report

This letter is in response to the draft findings of the audit that was preformed for the Town of Plattekill. I would like to thank the State Comptroller's audit team. The Comptroller's office recommendations will support our endeavors to operate in a manner that best serves the Town of Plattekill and the residents.

We obtained an understanding of internal controls that we deemed significant within the context of the audit.

- As of December, 2025 the unneeded network accounts have since been disabled.
- Town of Plattekill has made it mandatory for Cyber Awareness Training that is held through the year and made available via online training for all employees that have access to the network.
- In February of 2025 the Town of Plattekill adopted the Data Breach Policy that complies with Section 208 of the States Technology Law.
- The Town has been working with our IT company to assist in creating a contingency plan to help minimalize the risk of data loss or suffering a serious interruption of service.

Beyond these clarifications, the Town of Plattekill agrees with the auditors' recommendations and will provide a CAP that addresses them all.

Thank you,

Michael Lembo
Town of Plattekill Supervisor

P.O. BOX 45, 1915 RTE 44-55, MODENA, NY 12548
(845) 883-7331 FAX (845) 883-7207

Appendix C: Audit Methodology and Standards

We obtained an understanding of internal controls that we deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of our work on internal controls, as well as the work performed in our audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We reviewed the Town's IT policies and procedures, interviewed Town officials and employees and communicated with the IT service provider to gain an understanding of the Town's IT environment, including how Town officials managed network user accounts and whether the Town had a breach notification policy, an IT contingency plan, IT security awareness training and a contract or SLA with the IT service provider.
- We ran a computerized audit script on the domain controller on August 12, 2024 to determine the Town's enabled network user and computer accounts. We identified 28 enabled network user accounts and compared them to a list of current employees to identify whether any accounts were assigned to former Town employees. We followed up with the confidential secretary to determine which network user accounts were no longer needed and why any unneeded accounts remained enabled on the network.
- We requested all IT security awareness training certificates for Town employees and compared the names on the certificates received to the list of current employees to determine how many employees received the training. We interviewed the confidential secretary to determine which employees use the Town's computer network and documented whether they received IT security awareness training.
- We used a random number generator to randomly select a sample of 10 out of 77 employees from the employee list and requested their signed Handbook Acknowledgement forms indicating that they read or will read the handbook which includes the Town's IT policy.

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 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.

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 relevant population size and the sample selected for examination.

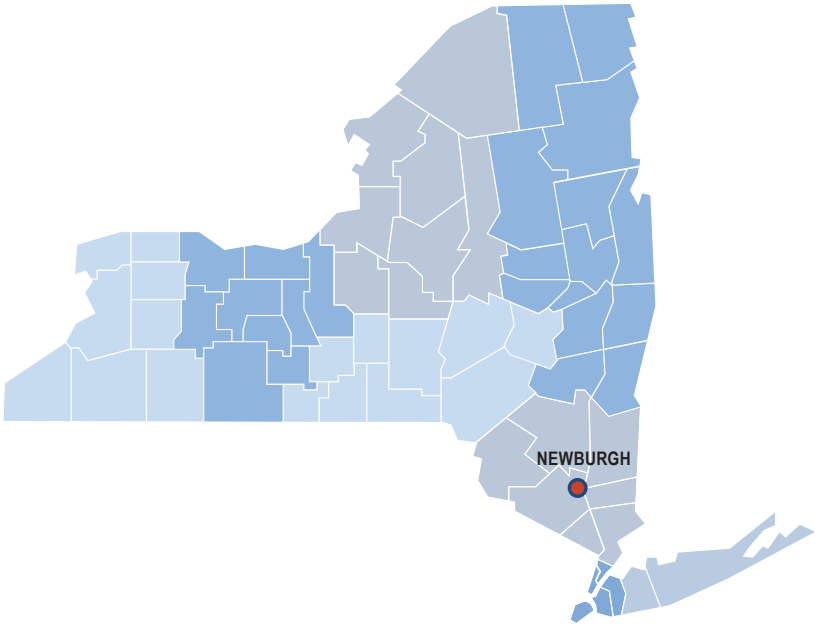
Contact

NEWBURGH REGIONAL OFFICE – James L. Latainer, Chief of Municipal Audits

33 Airport Center Drive, Suite 102 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.ny.gov

Serving: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester counties



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

https://www.osc.ny.gov/local-government

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