New York State Comptroller
THOMAS P. DiNAPOLI

Town of Horseheads

Information Technology

2025M-109 | February 2026

Division of Local Government and School Accountability

Contents

Audit Results

Town of Horseheads

Audit Objective	Audit Period
Did Town of Horseheads (Town) officials adequately manage network and local user accounts, develop an information technology (IT) contingency plan, and provide adequate IT security awareness training to staff?	January 1, 2024 – January 21, 2025 We extended our audit period through March 26, 2025, to review documentation supporting whether data backups were occurring.

Understanding the Audit Area

Town officials must manage network and local user accounts, create IT contingency plans and provide IT security awareness training. Security awareness training helps to protect personal, private and sensitive staff information (PPSI),[1] by training personnel on cybersecurity best practices and to recognize the signs of a security incident, which can significantly reduce the likelihood of a cyberattack succeeding, such as a phishing attempt. Unmanaged user accounts are potential entry points for attackers and other unauthorized individuals, and if compromised the lack of a contingency plan can paralyze a town's operations. In the event of a successful attack, security awareness training is also a compensatory control that can help reduce the risks of the attack, such as data breaches, financial loss or other issues, 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 against financial loss and ensure critical functions continue.

In calendar year 2024, the Town paid an outside IT vendor $14,790 to provide IT services, including IT support, network setup and maintenance, end point protection, managing user accounts and permissions and other IT-related services. The Town had 28 enabled network user accounts and five enabled local user accounts on the four computers reviewed.

[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.

Audit Summary

Town officials did not adequately manage network and local user accounts, develop and adopt a written IT contingency plan, or provide IT security awareness training to staff. Although the Town Board (Board) paid $14,790 to an IT vendor for IT-related services, it cannot be assured that the Town's IT systems are secured from unauthorized use and access, or that critical data would be preserved if an interruption in operations occurred since Town officials lack the necessary guidance to minimize potential damage and restore operations. The Board and Town officials did not:

- Adequately manage all network and local user accounts,
- Enter a written contract or service level agreement (SLA) with the IT vendor,
- Develop and adopt a written IT contingency plan, or
- Provide adequate IT security awareness training to staff.

The report includes five recommendations that, if implemented, will improve Town officials' oversight of IT processes. Sensitive IT control weaknesses were communicated confidentially to Town officials. 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 State Comptroller's 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 Town Clerk's office.

Information Technology: Findings and Recommendations

A town board should have a comprehensive written contract with its IT vendor that indicates the contract period, services provided and a compensation rate for those services. Additionally, a town board should have a written SLA with its IT vendor that identifies a town's needs and expectations and specifies the level of services provided.

To minimize the risk of data loss or service interruption in the event of an unexpected IT disruption or disaster, a town board and officials should develop and adopt a comprehensive written IT contingency plan.

Routine IT security awareness training helps ensure that personnel understand their responsibilities and procedures for safeguarding town data from potential abuse or loss. Such training should include key security concepts that include the dangers of downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured wireless network connections; and how to respond if a computer virus or an information security breach is detected.

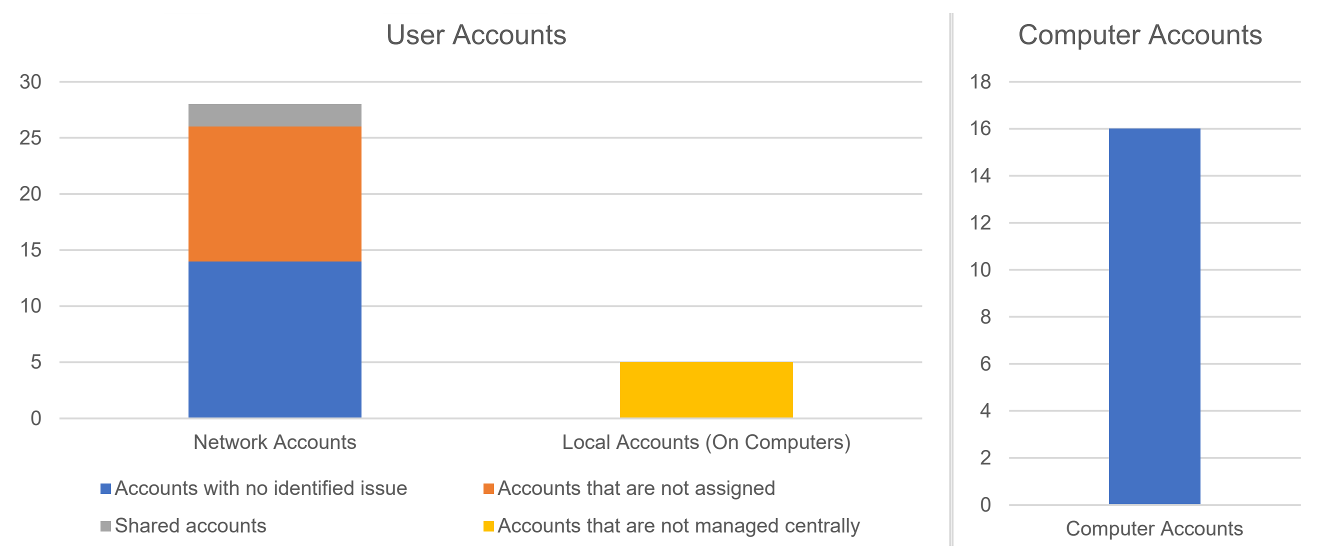
More details on the criteria used in this report, as well as resources/publications we make available to local officials that can help officials improve operations (Figure 3) are included in Appendix A.

Finding 1 – Town officials did not adequately manage network and local user accounts.

The Town did not have written procedures or a written Board-approved policy for user account management. We reviewed all 28 enabled network user accounts with access to the Town's network and identified 12 accounts that were not assigned to personnel and two accounts shared by multiple personnel. Additionally, we examined all 16 computer accounts[2] and all five local user accounts on the four computers reviewed (Figure 1). One computer had two local accounts.

[2] A computer account functions as an internal record within a network and allows IT administrators to manage computers using a centralized network management tool. Audit results related to computer accounts were communicated confidentially.

Figure 1: User and Computer Accounts Reviewed



Without controls to assign users properly and restrict accounts to a single person, this can create accountability concerns.

User Accounts[3] – Town officials did not ensure that user accounts were appropriately provisioned[4] or deprovisioned. For example, two of the 12 generic network user accounts were shared by six Town employees; one of these accounts had not been used in 2.5 years, while the other had never been used since its creation over 4.5 years ago. Nine accounts were not assigned to any specific individual or employee and the remaining account was assigned to the IT vendor.

Additionally, five of the 13 network user accounts were originally assigned to employees who left Town employment between 1.5 and five years ago. All five accounts were still in use; four were accessed within the last six months and the fifth remained enabled but was last used over a year ago.

Furthermore, three of the five local user accounts had generic usernames. One account had never been used, and the other two (both with local administrative privileges) were last used between one and four years ago.

The Town Supervisor (Supervisor) told us that Town officials did not rename network or local user accounts when employees left due to the associated costs and that accounts were shared to allow any of the six individuals to collect or enter data as needed. Additionally, Town officials did not have written procedures or a written Board-approved policy for user account management.

[3] A network user account can only access network resources from a computer with an associated network computer account. In addition, a local user account is stored on a server or computer and can only be used to log onto and access resources on that server or computer.

[4] Provisioning is the process of managing and maintaining users and their access rights to a town's systems.

Unused and unnecessary network user accounts are additional entry points into a network and, if accessed by attackers, could be used to inappropriately access and view PPSI accessible by those accounts and potentially compromise IT resources. Additionally, when multiple people use the same account, it can become challenging to attribute actions to a specific user and to investigate security incidents effectively.

IT Contracts – In calendar year 2024, the Town paid the IT vendor a total of $14,790 for covered services including software and hardware setup and maintenance, data backup support, antivirus monitoring, technical issue troubleshooting, identity and access management system configuration and user access provisioning. However, the Town did not have a written SLA or contract with the IT vendor that clearly defined responsibilities, identified the Town's needs and expectations and specified the level of services provided.

Not having SLAs or written contracts can contribute to confusion regarding who is responsible for various aspects of the IT environment, which puts data and IT systems at greater risk for unauthorized access, misuse or loss. Furthermore, Town officials cannot be assured that access to Town resources is appropriately provisioned and deprovisioned.

Recommendations

The Board and Town officials should:

1. Develop and adopt written policies and procedures for managing network and local user accounts that include periodically reviewing user access and disabling unneeded/or unused accounts and distribute the procedures to applicable staff and ensure that personnel implement and comply with the procedures.
2. Ensure that a comprehensive written contract and SLA are established with the IT vendor, clearly defining the contractual relationship and responsibilities of both the vendor and the Town.

Finding 2 – The Board did not develop or adopt a comprehensive written IT contingency plan.

The Board and Town officials did not develop or adopt a comprehensive, written IT contingency plan to document and inform staff how they should respond to unplanned disruptions and disasters that affect the Town's IT environment. The Supervisor told us that Town officials relied on a written regional emergency preparedness plan developed by a local municipality. We determined the emergency plan did not address specific procedures to recover from, or respond to, an IT-related disruption or disaster such as a ransomware attack or other unplanned event.

The IT vendor was responsible for performing nightly backups of all data, applications and operating systems. According to the Supervisor and a Town employee, the Town historically depended on the IT vendor's quick response to restore operations in a timely manner during service disruptions. We reviewed documentation and confirmed that backups were occurring and that a backup had been successfully restored. Although the IT vendor offered input on the Town's likely response to an unplanned event, the absence of a comprehensive written IT contingency plan leaves Town officials without adequate documented guidance to recover data, resume essential operations promptly and minimize damage and recovery costs.

Recommendation

3. The Board and Town officials should develop and adopt a comprehensive, written IT contingency plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

Finding 3 – Town officials did not provide IT security awareness training to staff.

None of the 18 Town employees with access to the Town's IT network completed IT security awareness training. The Board also did not adopt an IT security awareness training policy. The Supervisor told us that the Board is developing a technology policy and procedures to address training and other IT areas.

Routine IT security awareness training would ensure that personnel understand their responsibilities and procedures for safeguarding Town data from potential abuse or loss. Personnel who have not received recurring and routine training may be more vulnerable to cybersecurity threats. By not providing IT security awareness training, the Town is at an increased risk of data loss and significant operational disruptions in the event of a cyber incident or other IT-related event.

Recommendations

The Board should:

4. Develop and adopt a written IT security awareness policy and ensure that all personnel receive routine IT security awareness training.

5. Routinely communicate cybersecurity expectations to Town officials and employees.

Appendix A: Profile, Criteria and Resources

Profile

The Town, located in Chemung County, is governed by the elected five-member Board composed of the Supervisor and four Board members.

The Board is responsible for the general oversight of the Town's operations and finances, which includes maintaining security over the Town's IT system. The Town has 44 employees, 28 enabled network user accounts, five local user accounts enabled on four computers (one computer had two local accounts) and 16 network computer accounts (i.e., servers, desktops and laptops).

Criteria – IT

A town's IT systems and the data stored within are valuable and need to be protected from unauthorized access, inappropriate use or loss. A town board should establish IT policies that consider people, processes and technology. A town board should communicate these policies to all computer users, ensure town officials develop procedures to monitor compliance with IT policies and ensure that personnel receive routine IT security awareness training.

Although no single practice or policy on its own can adequately safeguard IT systems from cybersecurity risks, there are several IT governance efforts that, if properly enacted and monitored, collectively increase the odds that IT systems will remain safe.

Network user accounts are necessary to allow authorized users access to resources on a server or computer on the network. Network user accounts are accounts that are assigned to employees, town officers, third-party vendors and/or shared users.[5] Although network user accounts can be set to limit access to certain resources, they are additional entry points into a network and could be used to inappropriately access unauthorized data and information. Effective account management involves establishing written procedures that guide network and/or system administrators in properly creating, granting, modifying and disabling user account access to a network. These procedures should specify the roles and responsibilities of employees and vendors and require periodic monitoring of all enabled network user accounts to help town officials determine whether the accounts are necessary and appropriate. All network user accounts should be disabled when they are no longer needed. Town officials should periodically review all network user accounts to determine whether they are necessary and identify any unused or infrequently used network user accounts (e.g., not used for six months or more).

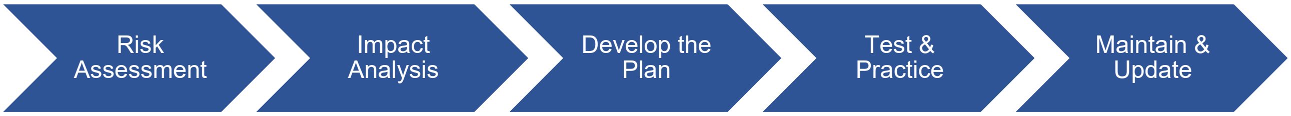
[5] Shared accounts are used by more than one user to log in to a computer system and access network resources. For example, shared accounts may be used for testing processes, training purposes or shared email accounts.

When possible, town officials should establish a unique individual user account for each user to provide accountability. While managing network user accounts, town officials should limit the use of shared network user accounts because they are not linked to one individual, and users may not be held individually accountable for their actions when using these accounts. Shared user accounts should be routinely reviewed to determine whether they are necessary.

A town board should have a comprehensive written contract and SLA with its IT vendor that clearly defines the terms of the relationship and the responsibilities of both the vendor and the town. An SLA establishes comprehensive, measurable performance targets so that there is a mutual understanding of the nature and required level of services the vendor will provide. Having a written contract and SLA with the IT vendor will allow town officials to monitor the IT vendor's work to ensure that the town is receiving all contracted services.

An IT contingency plan should begin with a risk assessment, followed by an impact analysis, which assesses the effects of the identified risks. A plan should then be developed to address these effects, regularly tested to ensure its effectiveness and updated as needed (Figure 2).

Figure 2: The IT Contingency Plan Lifecycle



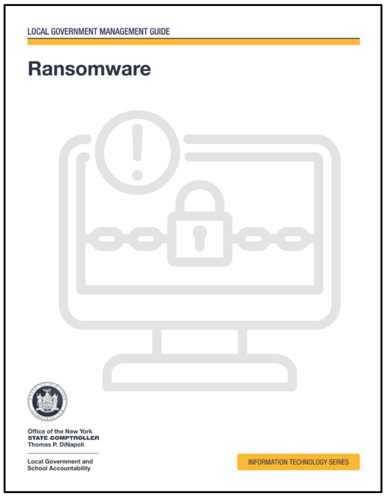
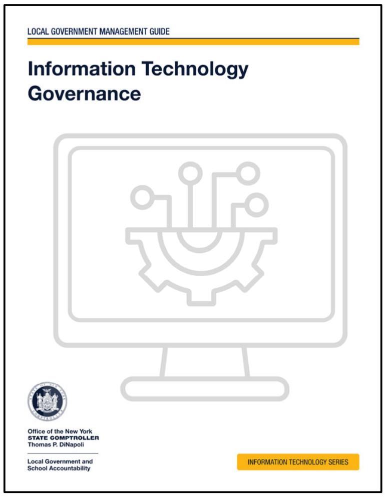
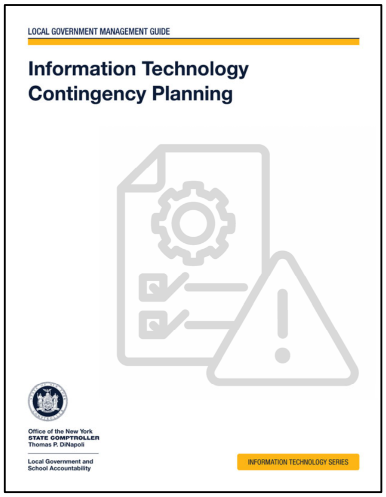
Typically, IT contingency planning involves analyzing business processes and continuity needs, focusing on sustaining critical functions and identifying roles of key individuals and necessary precautions needed to maintain or quickly resume operations. The plan should be periodically tested and updated to ensure town 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 help ensure backups will function as intended.

To help minimize the risk of disruption, town officials should receive periodic IT security awareness training that explains common security threats and the proper rules of behavior for using the Internet and IT resources, systems and data. The training should communicate policies and procedures to all IT system users so they understand IT security measures and their roles in safeguarding data and IT assets. Such training should include key security concepts such as the dangers of downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured wireless network connections; and how to respond if a computer virus or an information security breach is detected.

Additional IT Resources

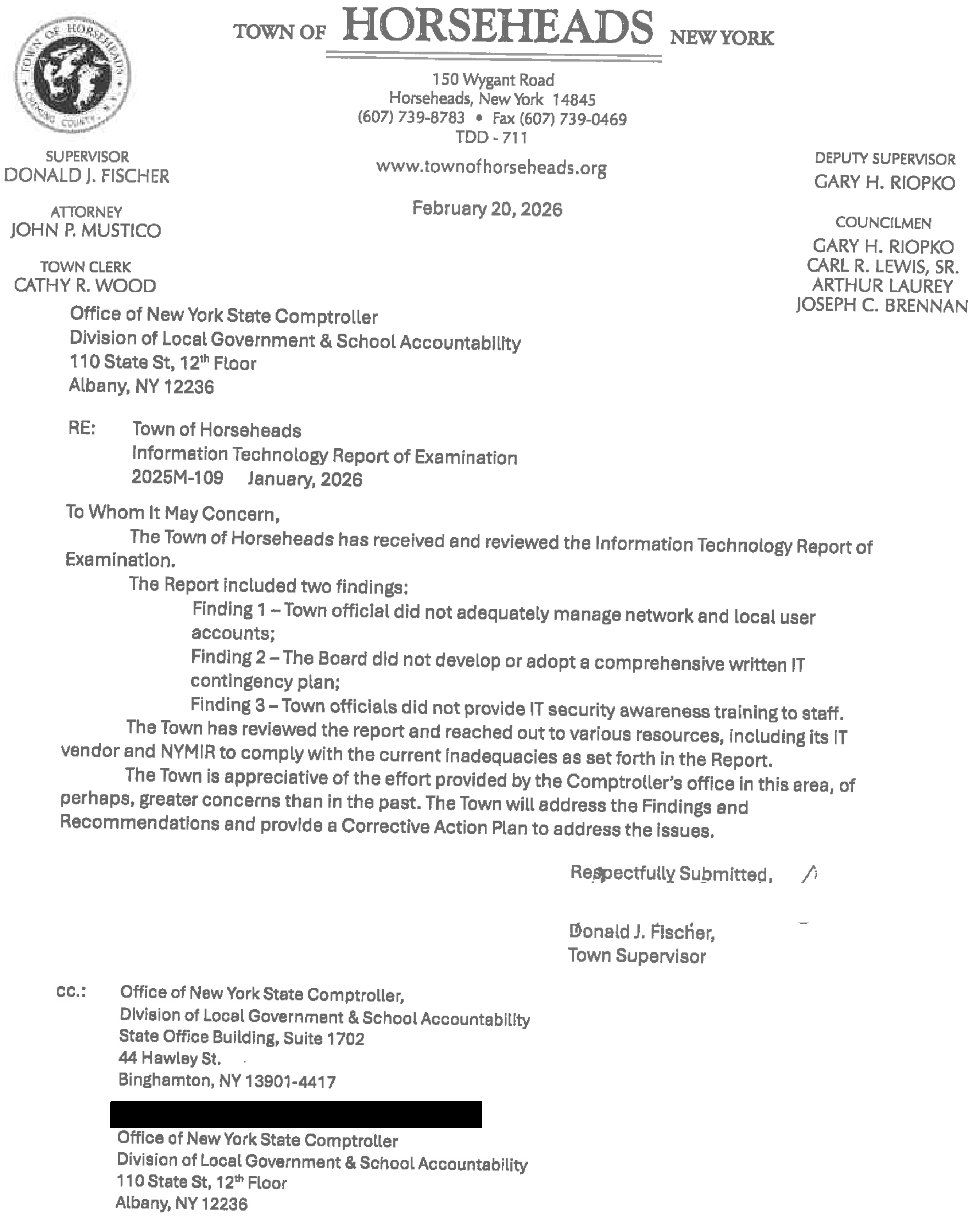
Figure 3: OSC Publications

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

Ransomware	***Information Technology Governance***	***Information Technology Contingency Planning***
 LOCAL GOVERNMENT MANAGEMENT GUIDE Ransomware Office of the New York STATE COMPTROLLER Thomas P. DiNapoli Local Government and School Accountability INFORMATION TECHNOLOGY SERIES	 LOCAL GOVERNMENT MANAGEMENT GUIDE Information Technology Governance Office of the New York STATE COMPTROLLER Thomas P. DiNapoli Local Government and School Accountability INFORMATION TECHNOLOGY SERIES	 LOCAL GOVERNMENT MANAGEMENT GUIDE Information Technology Contingency Planning Office of the New York STATE COMPTROLLER Thomas P. DiNapoli Local Government and School Accountability INFORMATION TECHNOLOGY SERIES
https://www.osc.ny.gov/files/local-government/publications/pdf/ransomware.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 HORSEHEADS NEW YORK

150 Wygant Road
Horseheads, New York 14845
(607) 739-8783 • Fax (607) 739-0469
TDD - 711

www.townofhorseheads.org

SUPERVISOR
DONALD J. FISCHER

ATTORNEY
JOHN P. MUSTICO

TOWN CLERK
CATHY R. WOOD

DEPUTY SUPERVISOR
GARY H. RIOPKO

COUNCILMEN
GARY H. RIOPKO
CARL R. LEWIS, SR.
ARTHUR LAUREY
JOSEPH C. BRENNAN

February 20, 2026

Office of New York State Comptroller
Division of Local Government & School Accountability
110 State St, 12th Floor
Albany, NY 12236

RE: Town of Horseheads
Information Technology Report of Examination
2025M-109 January, 2026

To Whom It May Concern,

The Town of Horseheads has received and reviewed the Information Technology Report of Examination.

The Report included two findings:

Finding 1 – Town official did not adequately manage network and local user accounts;

Finding 2 – The Board did not develop or adopt a comprehensive written IT contingency plan;

Finding 3 – Town officials did not provide IT security awareness training to staff.

The Town has reviewed the report and reached out to various resources, including its IT vendor and NYMIR to comply with the current inadequacies as set forth in the Report.

The Town is appreciative of the effort provided by the Comptroller's office in this area, of perhaps, greater concerns than in the past. The Town will address the Findings and Recommendations and provide a Corrective Action Plan to address the issues.

Respectfully Submitted,

Donald J. Fischer,
Town Supervisor

cc.: Office of New York State Comptroller,
Division of Local Government & School Accountability
State Office Building, Suite 1702
44 Hawley St.
Binghamton, NY 13901-4417

[redacted]
Office of New York State Comptroller
Division of Local Government & School Accountability
110 State St, 12th Floor
Albany, NY 12236

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 interviewed Town officials, employees and the IT vendor to obtain an understanding of the Town's IT operations and related policies and procedures and to determine whether the policies and procedures were adequate, an IT contingency plan was in place, an SLA had been established and Town employees had received IT security awareness training. We also reviewed the Chemung County regional emergency preparedness plan the Town relied on to determine whether it included specific procedures for responding to an IT-related disruption.

- We selected the Town's server and a sample of four computers because of the likelihood that they contained PPSI or other sensitive information. We ran a computerized audit script on the server and three of the computers on January 8, 2025, and on one computer on January 21, 2025. We analyzed the resulting reports to identify potential weaknesses in the Town's network and local user account management. Our review included all 28 enabled network user accounts, all 16 computer accounts and all five local user accounts enabled on the four sampled computers. We compared the users of these accounts to current employee and Town officials lists to identify any unused and potentially unnecessary accounts. We discussed all identified user accounts with Town officials.

- We reviewed all invoices paid to the IT vendor in calendar year 2024 to identify the services provided. We also reviewed documentation to determine whether data backups were performed and successfully restored.

This 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 the relevant population size and the sample selected for examination.

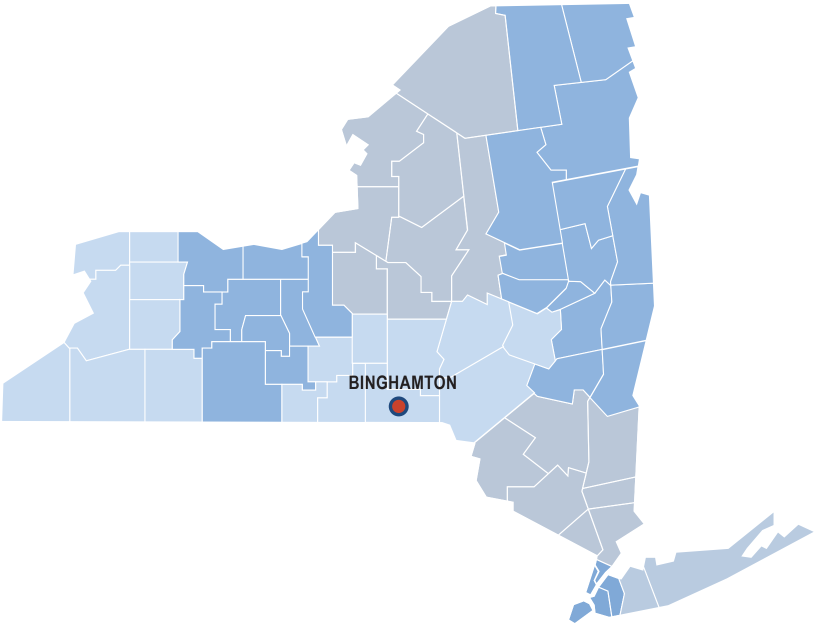
Contact

BINGHAMTON REGIONAL OFFICE – Lucas S. Armstrong, Chief of Municipal Audits

State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417

Tel (607) 721-8306 • Fax (607) 721-8313 • Email: Muni-Binghamton@osc.ny.gov

Serving: Broome, Chemung, Chenango, Cortland, Delaware, Otsego, Schoharie, Tioga, Tompkins 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