New York State Comptroller
THOMAS P. DiNAPOLI

Village of Lacona

Cybersecurity

August 2026 | 2026M-23
Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Village of Lacona

Audit Objective

Did the Village of Lacona (Village) Board and Village officials (officials) provide adequate governance to safeguard information technology (IT) assets from cybersecurity threats?

Audit Period

June 1, 2024 – October 3, 2025

Understanding the Audit Area

Village officials should provide adequate cybersecurity governance to protect IT assets; ensure operational continuity; safeguard personal, private or sensitive information (PPSI);[1] reduce the risk of cyber incidents and financial losses; comply with legal obligations; and maintain public confidence.

Village officials engaged two external IT service providers during the audit period to perform various IT services, including hardware maintenance and repair, security services and other IT support services. The Village had six employees and three computers (two desktops and a laptop) as of October 2025.

Audit Summary

The Board and officials did not provide adequate governance to safeguard IT systems from cybersecurity threats. The Board and officials did not develop or adopt written IT policies, provide employees with cybersecurity awareness training or develop an IT contingency plan to help minimize the risk of data loss or suffering a serious operational interruption. As a result, the Board and officials cannot be assured that Village IT systems and PPSI contained therein are secured and protected from unauthorized use, access, manipulation and loss. The Board and officials also have minimal assurance that, in the event of a disruption or disaster (e.g., a ransomware attack), employees and other parties would be able to react quickly and effectively to help resume, restore and report critical IT systems failures or data breaches in a timely manner.

Without effective cybersecurity governance, including Board-adopted and enforced policies, clearly documented roles and responsibilities and cybersecurity awareness training, the Village is at an increased risk of a successful cyberattack. Cyberattack effects can include IT system downtime and disruption, the inability to provide services reliant on IT assets, data theft (exfiltration) or corruption by malicious actors, and increased remediation and recovery costs. Cybersecurity governance weaknesses may also lead to ineffective cybersecurity risk management and inefficient incident response, which could potentially result in unauthorized access to Village IT assets and data.

Sensitive IT control weaknesses were communicated confidentially to officials.

The report includes four recommendations that, if implemented, will improve the Village's cybersecurity governance and IT system safeguards. Village officials agreed with our findings and recommendations and indicated they plan to initiate corrective action.

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.

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. 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 the New York State 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 Village Clerk-Treasurer's (Clerk-Treasurer) office.

Cybersecurity: Findings and Recommendations

The village board and village officials should treat cybersecurity risks as they do any other hazards they encounter: identify the risks, reduce their vulnerabilities and plan for contingencies. This requires an investment of time and resources and a collaborative work environment among the village board, officials and others responsible for managing and securing a village's IT systems. Many cybersecurity vulnerabilities can be mitigated with no or minimal additional cost. It is imperative that village officials partner together to address cybersecurity risks and help protect IT assets from prevalent and emerging threats.

Village officials should provide cybersecurity awareness training to ensure employees understand IT security measures, their responsibilities and how to safeguard data from potential misuse or loss. Policies and training help define and communicate the expectations for appropriate IT user behavior and explain the consequences of policy violations. Therefore, it is essential for a village board to adopt, update and distribute policies for key cybersecurity issues to help safeguard from cybersecurity threats including unauthorized access, use or loss.

The village board should periodically review cybersecurity policies, update them as needed and establish who is responsible for monitoring compliance with these policies. Cybersecurity policies describe the tools and procedures used to help protect IT systems, including the data contained therein, from cybersecurity threats. Additionally, the village board should also ensure a comprehensive written IT contingency plan is developed and implemented to help minimize the risk of data loss or suffering a serious operational interruption in the event of an unexpected IT disruption or disaster.

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

Finding 1 – The Board did not adopt cybersecurity policies or provide cybersecurity awareness training.

The Board did not adopt written cybersecurity policies during the audit period or in prior years. Therefore, it did not provide adequate guidance and direction to address key cybersecurity issues, such as acceptable use of Village IT resources and expectations for selecting and using strong passwords. An acceptable use policy (AUP) outlines acceptable behaviors, responsibilities, and consequences for employees and vendors using Village IT equipment. In addition, Village officials did not provide cybersecurity awareness training to help ensure employees understand cybersecurity measures, their responsibilities and how to safeguard data from potential misuse or loss.

Because the Board did not adopt an AUP governing the appropriate use of IT assets, or provide employees with cybersecurity awareness training, we reviewed Internet browsing histories on all three Village computers.[2] While we did not identify any significant personal Internet use by Village officials or employees, without an AUP to proactively define user responsibilities and training to demonstrate due diligence and compliance, there is an increased risk that employees may browse the Internet or conduct other Internet activity that could expose Village IT systems to cybersecurity threats including malicious software infections or data breaches.

The Mayor told us that he is aware of the need to adopt comprehensive cybersecurity policies and procedures. However, with the turnover of elected and appointed officials, along with the small size of the Village's IT environment, the development and adoption of policies and procedures was overlooked. Village officials also relied on the IT vendor to perform the Village's IT functions (e.g., device management and email security). Although the contract between the Village and the IT vendor included a provision for cybersecurity awareness training, Village officials did not request the training materials. Therefore, Village employees were not provided

2 See Appendix C for our audit methodology.

the training. In addition, because the Village lacked cybersecurity policies and procedures, the IT vendor relied on its internal cybersecurity policies and practices to support the Village's IT systems.

While comprehensive policies will not guarantee the safety of IT assets and data, without adopting policies and providing cybersecurity awareness training, the risk significantly increases that users may not understand their responsibilities and are more likely to be unaware of situations that could put Village data and PPSI at greater risk for unauthorized access, misuse and loss. For example, if a user inadvertently downloaded a malicious software program from the Internet, or clicked on a malicious attachment, it could infect the user's computer and potentially infect other Village computers. This could allow individuals to steal information or gain unauthorized access to sensitive information in Village custody, such as employees' or residents' Social Security numbers disrupting daily operations such as payroll.

Recommendations

The Board should:

1. Adopt and communicate written cybersecurity policies and procedures, including an AUP, to Village employees.

The Mayor should, with the assistance of the Clerk-Treasurer as needed:

2. Develop and implement written procedures to monitor compliance with Board-adopted cybersecurity policies.

3. Ensure cybersecurity awareness training is periodically provided to all employees who use Village IT resources.

Finding 2 – The Board and Village officials did not develop and implement an IT contingency plan.

The Board and Village officials did not develop and implement an IT contingency plan to describe the procedures to recover from an unexpected IT disruption. The Mayor told us that they rely on the IT vendor to perform IT functions and was unaware of the necessities of an IT contingency plan.

A written IT contingency plan is critical to cybersecurity governance because it provides a structured approach to mitigating a cybersecurity disruption's resulting impacts, thus minimizing damage, reducing recovery time and costs, and helping to avoid legal or reputational repercussions. Without an approved and adopted IT contingency plan, responsible parties may not be aware of the steps they should take or how to continue doing their jobs to resume business in the event of a disruption or attack (e.g., ransomware), in a timely manner. In addition, there is an increased risk that the Village could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees.

Recommendation

The Board should:

4. Direct the Clerk-Treasurer to work with the IT vendor to develop a comprehensive written IT contingency plan for the Board's approval and adoption, ensuring the approved plan is implemented and distributed to all responsible parties, routinely tested and updated as needed.

Appendix A: Profile, Criteria and Resources

Profile

The Village, located in the Town of Sandy Creek in Oswego County, is governed by an elected three-member Board that includes the Village Mayor and two Board members. The Village has 657 residents.

The Village shares a common geographical boundary with the Village of Sandy Creek and the two Villages cooperatively share services, including the contracts for the third-party IT vendor and financial application services. The IT vendor is responsible for managing the Village's IT assets, setting up networks, user accounts and additional computers as needed, installing software, managing virus protection and any other Village IT-related needs, such as providing cybersecurity awareness training materials by request. The other vendor provides accounting software and support including maintenance and troubleshooting.

The Board is responsible for the general oversight of the Village's operations, which includes ensuring safeguards for the Village's IT system and fiscal overview. The Mayor is responsible for ensuring cybersecurity policies, guidelines and procedures are implemented effectively. The Clerk-Treasurer is responsible for day-to-day operations, ensuring that necessary services provided by the IT and financial application vendors are functioning as intended.

Village officials and employees use Village-owned IT assets (e.g., computers, laptops and tablets) to perform day-to-day operations and access stored information collected by the Village. The Village relies on its IT assets for Internet access, email and maintaining various records, such as financial and personnel records and other information that may contain.

Criteria

Although no single practice or policy on its own can adequately safeguard IT systems from cybersecurity threats, there are several cybersecurity governance efforts that, if properly enacted and monitored, collectively increase the odds IT systems will remain safe. A village board should provide oversight and leadership by adopting cybersecurity policies that consider people, processes and technology. These policies should be communicated to all IT system users and include procedures to ensure compliance. This helps reduce the risk of data, hardware and software being lost, damaged or compromised by unauthorized access and misuse.

Village officials should provide periodic comprehensive cybersecurity awareness training to help minimize the risk of unauthorized access to IT systems and the misuse or loss of confidential data. Cybersecurity awareness training should explain rules of behavior for using the Internet and Village IT resources and communicate related policies and procedures to all IT users. IT system 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 cybersecurity policies provide guidance for IT users, cybersecurity awareness training helps users understand their roles and responsibilities to ensure electronic data is protected. Training programs should be tailored to the specific audience (e.g., system users or administrators) and include guidance on how to perform their tasks while protecting electronic data. Cybersecurity awareness training should reinforce cybersecurity policies and focus on general security or specific risks such as the dangers of opening unknown emails, attachments or downloading files from the Internet.

In addition, the village board should ensure a comprehensive written IT contingency plan is developed and implemented to help minimize the risk of data loss or suffering a serious operational interruption 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 confidentiality, integrity or availability of village services,

including the IT system and data. 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 to maintain or quickly resume operations. The plan should be periodically tested and updated to ensure village 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.

Additional Resources

OSC *Local Government Management Guides* and other informational resources that are available on our website to help officials understand and perform their responsibilities include:

- ***Information Technology Governance:***
  https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf

- ***Information Technology Contingency Planning:***
  https://www.osc.ny.gov/files/local-government/publications/pdf/itcontingencyplanning.pdf

- ***New York Local Government and School Cybersecurity: A Cyber Profile:***
  https://www.osc.ny.gov/files/local-government/publications/pdf/nys-local-gov-school-cyber-profile.pdf

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

Appendix B: Response From Village Officials

The content below is a reproduced copy of the original response letter issued by Village officials and is reformatted to meet the Americans with Disabilities Act *Web Content Accessibility Guidelines (WCAG)*,[3] and may have included changes to spelling and grammar. The substance of the content was not changed.

Village of Lacona
11 Park Avenue
PO Box 217
Lacona, New York 13083-0217
Telephone (315} 387-5564

July 29, 2026

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

Attention: Jennifer Kenneson, Chief Information Systems Officer

Re: Village of Lacona Preliminary Draft Findings, Examination 2026M-23

Ms. Kenneson,

On July 22, 2026, we reviewed the Draft Cyber Security Report with your audit team. After a discussion about the draft audit in general, specifically the Audit Summary and the Audit Findings and Recommendations, I was asked by the Supervisor if I agreed with the findings. My reply was yes, I do agree with the findings and recommendations of the Draft Report.

Since that meeting I have reached out to both our IT vendors and our insurance carrier. I am certain that between the templates provided by your cyber security audit team, the links provided in the draft report, our carrier's cyber security risk specialist and our vendors, we will be able to implement the audit's recommendations.

IT is certainly not my area of expertise and I found the interaction with the audit team educational and non-judgmental. I felt this was a good experience and learning opportunity for the Village.

Very truly yours,

Steven D. Haskins
Mayor

3 https://www.ada.gov/resources/2024-03-08-web-rule/#highlights-of-the-requirements-in-the-rule

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 Board members, Village officials, employees and the Village's third-party IT and financial application vendors to obtain an understanding of the Village's IT system operations and cybersecurity-related policies and procedures to determine whether the policies and procedures were adequate to safeguard from cybersecurity threats, an IT contingency plan existed, and the Board, Village officials and employees received cybersecurity awareness training.

- We ran a computerized audit script on the three employees' computers on October 3, 2025, and reviewed the Internet history exported by the script to evaluate whether Internet use was appropriate and whether unnecessary exposure of PPSI may have occurred.

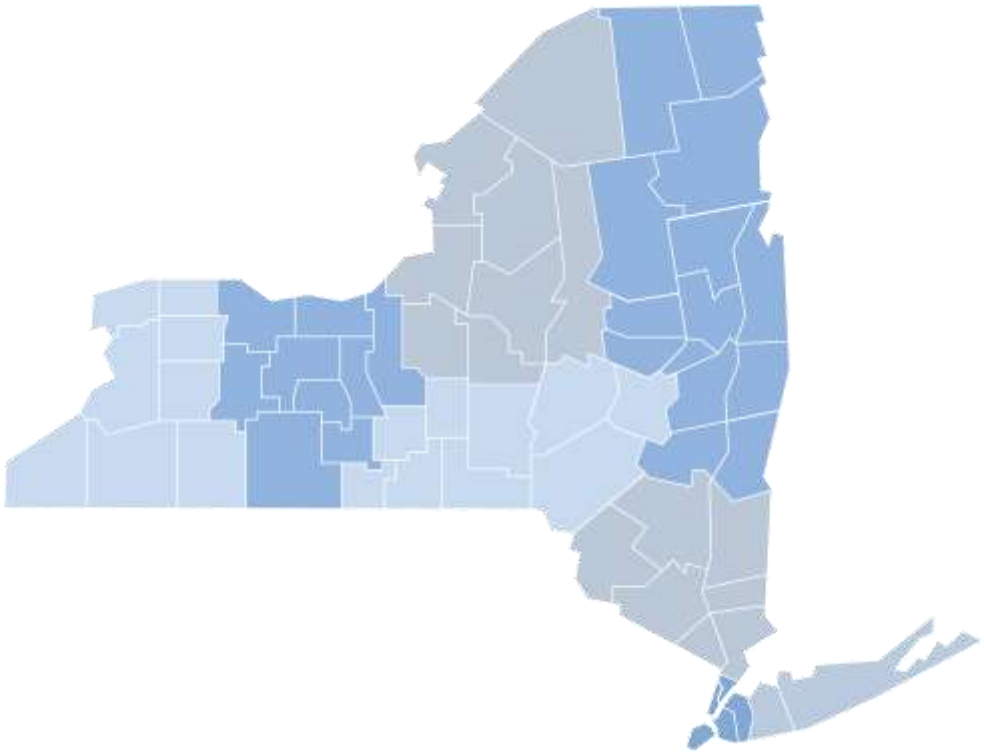
- We physically observed the Village's IT assets to determine whether the Board and Village officials implemented adequate physical security controls.

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 Village 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.

Questions?

APPLIED TECHNOLOGY UNIT
Jennifer Kenneson, Chief Information Systems Auditor
110 State Street, 12th Floor • Albany, New York 12236
Tel (518) 738-2639 • Fax (518) 486-6479
Email: Muni-Cyber@osc.ny.gov



Contact

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

(518) 474-4044

www.osc.ny.gov

Prepared by the Division of Local Government and School Accountability