New York State Comptroller
THOMAS P. DiNAPOLI

Village of Cassadaga

Cybersecurity

August 2026 | 2026M-25
Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Village of Cassadaga

Audit Objective

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

Audit Period

June 1, 2024 – October 1, 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 six external IT service providers during the audit period to perform various IT services, including printer support, hardware maintenance and repair, security services and other IT support services. The Village had eight full-time and 11 part-time employees and three computers as of October 2025.

Audit Summary

The Board and Village officials did not provide adequate governance to safeguard IT assets from cybersecurity threats. Because the Board and officials did not establish and maintain a comprehensive IT asset inventory, they could not effectively track these assets through their lifecycle. Additionally, policy, oversight and other internal control weaknesses increased the risk that IT assets and the data contained in IT systems could be lost, damaged or compromised. As a result, the Village's financial data and other PPSI was at increased risk of unauthorized use, access, manipulation and loss, which could lead to financial loss and operational interruptions.

Without effective cybersecurity governance, including Board-adopted and enforced policies and IT contingency plan, 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 eight recommendations that, if implemented, will improve the Village's cybersecurity governance and IT asset safeguards. Village officials agreed with our findings and indicated they plan to initiate corrective action.

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.

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.

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 Clerk-Treasurer's office.

Cybersecurity: Findings and Recommendations

The village board and officials should treat cybersecurity risks, as they do any other hazards they encounter, by identifying the risks, reducing their vulnerabilities and planning 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 against prevalent and emerging threats.

The village board should adopt comprehensive written policies that set forth guidelines and procedures for establishing and maintaining IT asset inventories. In addition, village officials should review IT asset inventory records to determine whether IT assets are needed and document and update the inventory for asset disposal.

Village 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, the village board should enter into formal written contracts and service level agreements (SLAs) with IT service providers that sufficiently define the contractual relationship and responsibilities between both parties.

The village board must adopt a breach notification policy that details actions to be taken to promptly notify affected individuals of a data breach if PPSI 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. The village board should also adopt an acceptable use policy (AUP) for village IT assets to help ensure users are aware of the proper use of the assets.

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 and Village officials did not maintain an IT asset and software inventory or dispose of unused and unneeded IT assets and software.

Because Village officials did not maintain an IT asset inventory, they were not aware of an all-in-one printer/scanner (printer/scanner) stored at the Village's public works facility that should have been disposed of in 2017 (Figure 1) when it was replaced by the current printer/scanner.

The Clerk-Treasurer and Superintendent of Public Works (Superintendent) indicated they were unaware of this unused asset and did not recognize the risk that retaining it could pose to the Village's cybersecurity. Not disposing of the unused printer/scanner in a timely manner exposed the Village to cybersecurity threats because unauthorized access to the asset could lead to sensitive Village data being compromised, such as previously printed, copied or scanned financial records, reports or PPSI stored on the device during its previous use (i.e., printing, copying and scanning records and reports).

Figure 1: Unneeded All-in-One Printer Not Disposed of in a Timely Manner[2]

While Village officials maintained asset inventories for accounting and insurance purposes, the inventories were limited to assets valued over $5,000 (e.g., vehicles and buildings) and did not account for IT assets below this threshold.

Furthermore, the Clerk-Treasurer told us that a cloud-based file transfer program that we identified in audit testing was not needed but remained installed on a Village computer and was intended to be used for financial operations several years ago. However, cloud-based file transfer software can pose additional risks to the Village's cybersecurity because data may be uploaded or moved from the computer to the cloud without Village officials' awareness, leading to unauthorized data exfiltration and/or the computer being compromised.

The Clerk-Treasurer and Deputy Clerk told us they were unaware that the unused cloud file-transfer program was still installed on the computer and did not recognize the cybersecurity threat significance or need to remove it. We confirmed that Village officials uninstalled this software after our audit inquiry.

The Board and officials may have identified and properly disposed of the unused printer/scanner and cloud-based file transfer program in a timely manner had they established a policy to ensure a comprehensive IT asset and software inventory was maintained. An adequate IT asset and software inventory policy should define responsibilities and expectations for the Village's IT assets and software, including those that are cloud-based, and help the Board and officials to identify vulnerabilities, ensure functionality and confirm disposal. Because the Board and officials did not establish and maintain an IT asset inventory, they could not effectively track these assets from procurement and use to obsolescence and disposal. As a result, the Village's IT assets were at increased risk of loss, theft or unauthorized use.

2 Photo taken by OSC auditors in October 2025 with permission of Village officials.

Recommendations

The Board should:

1. Adopt a policy requiring complete, accurate and up-to-date IT asset and software inventories, and the disposal or removal of IT assets and software in a secure and timely manner when no longer needed or used.

2. Ensure Village officials develop and implement written procedures for maintaining an IT asset and software inventory, including identifying, tracking, updating and reviewing IT assets and software, and properly disposing of unused IT assets and software in a timely manner.

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

The Board and Village officials did not have an IT contingency plan to describe the procedures to recover from an unexpected IT disruption. While the Board and Village officials developed and maintained an Emergency Operations Plan (EOP) the EOP did not address all necessary procedures and contact information to be considered an adequate IT contingency plan. The EOP focused on natural disasters rather than IT disruptions and IT recovery. The Deputy Mayor and Village officials could not recall why an IT contingency plan was not created.

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

3. The Board and Village officials should modify the EOP, or develop and adopt a separate, comprehensive written IT contingency plan, to define the Village's response procedures, escalation protocols and responsibilities before, during and after cybersecurity disruptions. The EOP and/or IT contingency plan should be distributed to all responsible parties, periodically tested and updated as needed.

Finding 3 – The Board and officials did not establish adequate contracts and SLAs with third-party IT service providers.

While the Village received IT-related services from six third-party IT service providers during the audit period, we determined that the Village did not have contracts or SLAs with three IT service providers, as one vendor only provided invoices per incident and the other two vendors only provided receipts per order.

We reviewed the written contracts and SLAs for the three remaining IT service providers and determined that they were not adequately detailed to ensure the Village received all contracted services. Village officials told us that although they did not have a sufficiently detailed contract and SLA with one of the IT service providers, they had a verbal agreement for cybersecurity protections and services offered by that provider and believed a verbal agreement was adequate.

However, without detailed contracts and SLAs, the Board and Village officials do not have a clear understanding of the responsibilities of both the Village and the IT service providers. As a result, the Village

officials cannot be assured that the Village is protected in the event of a malicious or inadvertent cybersecurity incident impacting the Village's IT assets, potentially leading to service or operational continuity disruptions at the Village and/or significant and unexpected financial, legal or reputational repercussions.

Recommendation

4. The Board and Village officials should review, update or enter into written contracts and SLAs with each third-party IT vendor that sufficiently defines the roles and responsibilities of each party and addresses the Village's specific IT service needs.

Finding 4 – The Board did not require cybersecurity awareness training for Village officials and employees.

The Board did not adopt a policy to require cybersecurity awareness training or provide cybersecurity awareness training to Village officials and employees. The Superintendent told us Village employees are generally skeptical toward unknown or unsolicited email communications. While this mindset may provide certain protections against cybersecurity threats such as phishing,[3] due to the rapid pace of change in technology and cybercrime, skepticism should be reinforced through periodic cybersecurity awareness trainings to safeguard Village IT assets and PPSI. The Deputy Mayor and Clerk-Treasurer told us cybersecurity awareness training was not required or provided because it was not a priority and they were not aware of its importance. The impact of the lack of cybersecurity awareness training was demonstrated in weaknesses identified during our audit across various aspects of the Village's cybersecurity governance, including the lack of an IT asset and software inventory, IT contingency plan and inadequate written contracts or SLAs discussed in Findings 1, 2 and 3, as well as the lack of other key cybersecurity governance policies discussed in Finding 5.

The lack of cybersecurity awareness can defeat many, if not all, cybersecurity controls and may lead to unauthorized access and sensitive data theft (exfiltration). Without requiring and providing cybersecurity awareness training to Village officials and employees, the Board cannot be assured that the Village's IT assets are safeguarded from cybersecurity threats. Additionally, effective January 1 2026, annual cybersecurity awareness training is required by New York State Technology Law Section 103-F for municipal employees who use technology as part of their official job duties, including village employees.

Recommendation

5. The Board should adopt a policy requiring, at a minimum, annual cybersecurity awareness training for employees who use technology as a part of their official job duties and ensure all Village officials and employees comply with the policy.

Finding 5 – The Board did not adopt adequate cybersecurity governance policies.

The Board and Village officials relied on IT assets to deliver essential Village services and communicate with residents. However, the Board did not adopt adequate cybersecurity policies to provide governance for safeguarding IT assets from cybersecurity threats, including policies addressing breach notification, acceptable use and passwords.

- The Board adopted a data breach notification policy in 2014. However, it was inadequate because the Board has not updated the policy since it was adopted. As a result, the policy did not reflect current standards governing breach notifications involving State residents' private information. Without an

3 Cybercriminals pose as a legitimate party in an attempt to get victims to engage with malicious content or links, share personal or sensitive information, or infect computers with malware such as ransomware.

adequate breach notification policy, the Board and Village officials may not fulfill their legal obligation to notify affected individuals in a timely manner when private information is compromised or is reasonably believed to be compromised.

- The Board adopted an AUP in 2014. However, the AUP was inadequate because it provided minimal guidance regarding the appropriate use of Village IT assets, software and Internet access. For example, while the AUP prohibited unauthorized software installation and noted potential disciplinary action, the AUP did not adequately address areas key to cybersecurity governance, including monitoring for compliance with the AUP, user responsibilities or expectations related to data protection, personal use and incident reporting. An inadequate AUP may lead to inconsistent user behavior, unauthorized system use and increased exposure to cybersecurity threats, including malware infections and data breaches.

- The Board did not adopt a password security policy. As a result, the Board did not provide guidance to officials and employees communicating the importance of selecting and using strong passwords to access Village computers and software in helping to safeguard IT assets.

We discussed the lack of adequate cybersecurity policies with Village officials, and they told us they were not aware of the importance of the policies. However, developing and adopting clear, current policies is an immediate, cost-effective step the Board and officials should take to help protect taxpayer resources, maintain public trust and ensure reliable Village service delivery.

Recommendations

The Board should:

6. Update the data breach notification policy to remain current with applicable data protection laws and regulations, reflect evolving definitions, adhere to modified reporting timelines and address third-party responsibilities.

7. Update the AUP to clearly describe what constitutes the appropriate and inappropriate use of IT resources, outline compliance monitoring and enforcement mechanisms and address data handling and security expectations.

8. Adopt a password security policy that establishes expectations for officials and employees when selecting passwords. The policy should communicate current industry standards for password security, and define any requirements related to, for example, password comparisons and/or changes, invalid password attempt thresholds and password encryption.

Appendix A: Profile, Criteria and Resources

Profile

The Village, located in the Town of Stockton in Chautauqua County, is governed by an elected five-member Board that includes the Village Mayor and four Board members and serves 573 residents. The Board is responsible for the general oversight of the Village's operations and finances, which includes adopting policies to safeguard IT assets from cybersecurity threats. The Village relies on third-party IT service providers for primary IT support, including firewall, hardware, financial software, and smoke and fire alarm support. Village employees use Village-owned IT systems for Internet access, email and online banking, and the data used by Village employees (e.g., village payroll, real property taxes) is hosted on servers owned, operated and monitored by the third-party IT service providers. The Village had eight full-time and 11 part-time employees during the audit period, and four of these employees routinely used Village IT assets to perform their job duties.

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 PPSI.

Criteria

The village board should ensure village officials maintain an up-to-date and accurate inventory of all IT assets to help minimize the potential for loss of assets and the compromise of data stored on IT assets. This list should be reviewed when deciding whether an asset should be retired from use. If an IT asset is retired, it should be properly destroyed to provide assurance to the village board that any sensitive data contained within the asset is sufficiently inaccessible. The village board should also ensure officials maintain an up-to-date and accurate inventory of all software approved and used on village IT assets to help minimize the potential of unauthorized users accessing sensitive village data. This list should be reviewed when deciding whether software is no longer needed, when software should be updated, and whether unauthorized software has been installed and should be removed. Officials also should comply with any policy adopted by the village board that sets forth guidelines and procedures for establishing and maintaining an asset inventory.

The village board should develop and adopt a comprehensive written IT contingency plan to help minimize the risk of data loss or suffering 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, updated and communicated 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.

The village board should enter into separate written contracts and SLAs between the village and its third-party IT service providers that identifies the village's needs and expectations and specifies the level of services to be provided. Properly designed contracts and SLAs establish comprehensive, measurable performance targets so that there is a mutual understanding of the nature and required level of services to be provided, including those related to the confidentiality and protection of PPSI. Having written contracts and SLAs with third-party IT service providers allows village officials to monitor the service provider's work to ensure that the village is receiving all contracted services.

The village board should adopt a policy which ensures that periodic comprehensive cybersecurity awareness training is provided to village officials and employees who use technology as a part of their official job duties to help minimize the risk of unauthorized access to IT systems and the misuse or loss of confidential data, including PPSI. Cybersecurity awareness training should explain rules of behavior for using the Internet and the village's IT assets 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 and IT policies provide guidance for IT users, cybersecurity awareness training helps users understand their roles and responsibilities to ensure electronic data is protected. Where feasible, these 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 and IT policies and focus on general security or specific risks, such as the dangers of opening unknown emails and attachments or downloading files from the Internet.

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 and IT policies that consider people, processes and technology. These policies should be communicated to all IT asset 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.

The village board should adopt an AUP that defines the procedures for computer, Internet and email use. The policy also should describe what constitutes appropriate and inappropriate use of IT resources and the village board's expectations concerning personal use of IT equipment and user privacy. Monitoring compliance with AUPs involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity. Officials should monitor and analyze activities for signs of possible violations or imminent threats of violations of computer security policies, AUPs or standard security practices.

The village board should adopt a policy that establishes expectations for configuring password settings and for users selecting passwords. The password policy should communicate current industry standards for password security and define any requirements related to, for example, password comparisons and/or changes, invalid password attempt thresholds and password encryption.

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)*,[4] and may have included changes to spelling and grammar. The substance of the content was not changed.

Village of Cassadaga
22 Mill Street, P.O. Box 286
Cassadaga, New York 14718
Phone: 716-595-3007

Ms. Jennifer Kenneson

Audit Background
The Village of Cassadaga received a final draft related to the New York State Comptroller's Office cyber security audit, along with a confidential letter dated July 15, 2026. The audit was conducted and completed before the new administration took office in January 2026.

Administrative Changes
Since taking office, this administration has appointed a new Village Clerk, Deputy Clerk, and Department of Public Works Superintendent. The Board agrees with the findings in the completed audit and recognizes the importance of cyber security in protecting Village assets and the residents we are sworn to represent.

Meeting with Audit Representatives
On Tuesday, July 22, 2026, Village Clerk Sue Penhollow and I met with two representatives from the audit team. They reviewed the final draft with us and provided reference materials to help educate this administration as we make necessary improvements soon.

Steps Already Taken
In the first seven months of this administration, the Board has made significant progress in improving the administrative and efficiency of both the Village office and the Department of Public Works. These efforts include:

- Removing and destroying the 2017 printer located in the DPW building.
- Replacing the prior steno-notepad process **[Redacted]**.
- Changing logins and passwords to more secure methods than those used by the previous administration.
- Hiring an accounting firm to provide financial services and obtaining the firm's cyber security policy for Village records.

Next Steps
We will continue to strengthen the Village's cyber security practices by reviewing and updating the outdated 2014 policy to reflect current needs and standards. We will also develop a corrective action plan, and the Village Board is committed to attending training sessions that will also include Village employees.

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

Appreciation
We appreciate the professionalism and courtesy shown by the two representatives from the State Comptroller's Office. Their assistance is valuable to Village's working through this process.

Respectfully submitted,

Rudy Abersold
Mayor, Village of Cassadaga

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 Village's policies to determine whether the Board adopted key cybersecurity and IT-related policies and the policies were adequate. In addition, we reviewed the Village's EOP to determine whether it was sufficient to serve as an IT contingency plan in the event a disruption interrupted Village services reliant on IT assets and software.

- We interviewed Board members and Village officials and employees to gain an understanding of the Village's IT environment and other cybersecurity and IT-related procedures to determine whether the Board's cybersecurity governance and other controls for safeguarding IT assets, including providing cybersecurity awareness training, was adequate to safeguard from cybersecurity threats.

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

- We compiled, analyzed and assessed software installed on all three Village-owned computers in use during the audit period using a computerized audit script run on August 7, 2025 and August 14, 2025 to determine whether Village officials ensured only properly approved and up-to-date software was installed for Village use.

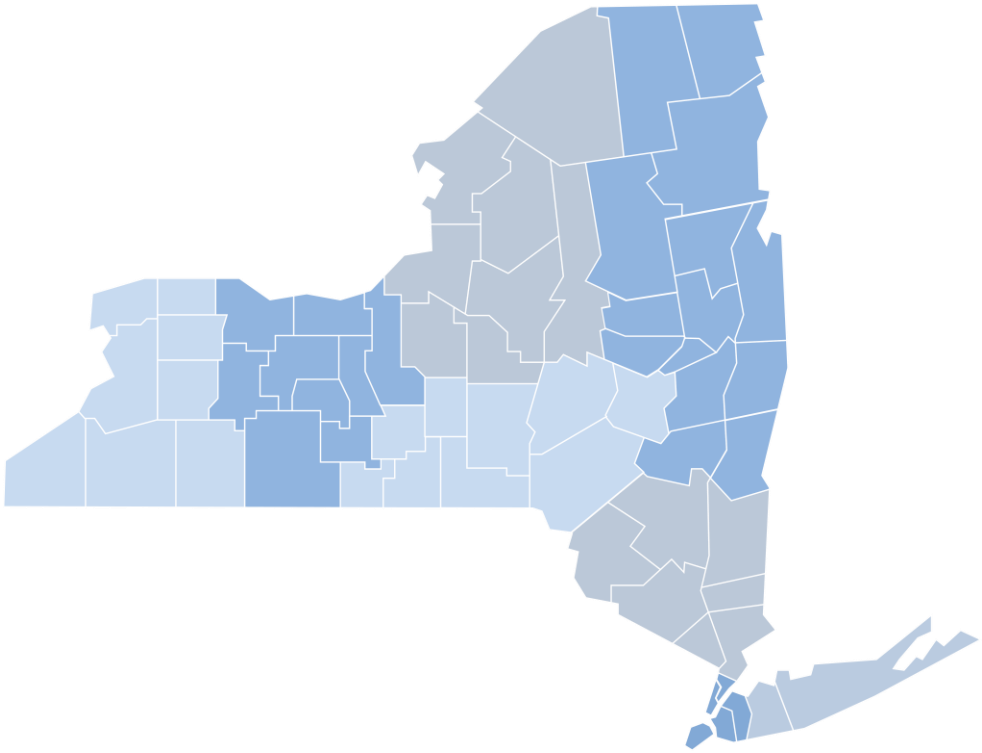
- We interviewed Village officials and employees to determine whether there were written contracts and SLAs between the Village and its third-party IT service providers, and if so, obtained a copy to determine whether the contracts and SLAs were adequate for the Village's IT environment. We also interviewed third-party IT vendor representatives to verify our understanding of the Village's contracts and SLAs.

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