New York State Comptroller
THOMAS P. DiNAPOLI

Town of Guilderland

Information Technology

2025M-61 | November 2025

Division of Local Government and School Accountability

Contents

Audit Results **1**

Audit Summary 1

Information Technology: Findings and Recommendations **3**

Finding 1 – Town officials did not monitor employee Internet use or provide IT security awareness training. 3

Recommendations 4

Finding 2 – Town officials did not implement strong access controls. 4

Recommendations 5

Finding 3 – The Board did not adopt an IT contingency plan or periodically test backups. 6

Recommendations 6

Appendix A: Profile, Criteria and Resources **7**

Appendix B: Response From Town Officials **9**

Appendix C: OSC Comment on the Town's Response **12**

Appendix D: Audit Methodology and Standards **13**

Audit Results

Town of Guilderland

Audit Objective	Audit Period
Did Town of Guilderland (Town) officials adequately secure and protect information technology (IT) assets against unauthorized use, access and loss?	January 1, 2024 – January 10, 2025

Understanding the Audit Area

Town officials and employees use Town-owned IT assets (e.g., computers, and laptops) to perform day-to-day operations and access and store information collected by the Town. The Town relies on its IT systems (including its IT assets and network) for Internet access and email, and to maintain various records, such as financial and personnel records, and evidence files for the police department, that may contain personal, private, or sensitive information (PPSI).[1] If an IT system is compromised, the results could range from inconvenient to catastrophic and may require extensive effort and resources to evaluate, repair and rebuild.

The Town has 228 enabled user accounts, 188 network computer accounts, 162 desktops and laptops and 31 servers.

Audit Summary

The Town Board (Board) and officials did not monitor employee Internet use or establish adequate controls to safeguard IT systems. In addition, the Board did not adopt an IT contingency plan to help minimize the risk of data loss or suffering a serious interruption of services, periodically test backups, or provide IT security awareness training. As a result, Town officials cannot be assured that Town IT assets are secured and protected against unauthorized use, access and loss, and there is an increased risk that officials could lose important data and suffer a serious interruption in operations.

The Town's technology use policy (IT Policy) prohibits employees from using Town-owned computers for personal use. However, within our sample of 14 Town computers, six users accessed websites for personal use, such as entertainment, news media, personal finance, email, shopping, travel, personal health and other miscellaneous personal use. In addition, one user conducted personal business activities using a Town computer.

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 multiple security weaknesses identified in the Town's IT systems, including inadequate access controls, compound the risk of a cyber disruption, including but not limited to, unauthorized use, access or loss of information maintained within the Town's IT assets.

Sensitive IT control weaknesses were communicated confidentially to officials.

The report includes seven recommendations that, if implemented, will improve the Town's IT practices to protect against unauthorized use, access and loss. Town officials generally agreed with our recommendations and have initiated or indicated they planned to initiate corrective action. Appendix C includes our comment on an issue raised in the Town's response letter.

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and New York Office of the 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 D.

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 GML Section 35. 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

A town's IT systems and the data they hold are valuable and need to be protected from unauthorized access, inappropriate and wasteful use or loss. A town board (board) should establish IT policies that consider people, processes and technology. Specifically, the board should ensure officials develop procedures to monitor compliance with the town's technology policy (specifying acceptable and prohibited computer system use), implement comprehensive procedures for managing and monitoring user access to the town's network and computers, adopt an IT contingency plan and deliver IT security awareness training.

More details on the criteria used in this report, as well as resources we make available to local officials to help improve operations (Figure 2), are included in Appendix A.

Finding 1 – Town officials did not monitor employee Internet use or provide IT security awareness training.

Although officials set up web filtering software to prevent access to certain websites, including obscene material and unlawful activity, they did not monitor employee Internet use.

We reviewed the Internet history on 14 Town computers (12 computers were assigned to 12 employees and the other two computers were shared computers) and determined that six users accessed websites for personal use. In addition, one user conducted personal business activities for their family-owned business using the Town computer (Figure 1).

Figure 1: Examples of Personal Internet Use

Type	Website
Entertainment and News Media	distro.tv, youtube.com, imdb.com, timesunion.com, msn.com, today.com
Personal Finance, Email and Shopping	venmo.com, chase.com, broadview.com, synchrony.com, gmail.com, aol.com, outlook.com, ulta.com, bestbuy.com, michaels.com, target.com
Travel	airbnb.com, southwest.com, delta.com, myrtlebeach.com
Personal Health	labcorp.com, trinityhealth.com, communitycare.com
Miscellaneous Personal Use	allmenus.com, toasttab.com, zmenu.com, quickpickpool.com, collegeboard.org, signupgenius.com
Personal Business	godaddy.com, chase.com, gmail.com

Town officials and employees are provided with an employee handbook which contains the Town's IT Policy. The IT Policy states employee computer access is solely for Town employment duties and prohibits any computer use unrelated to the employee's employment. Furthermore, officials and employees need to sign an acknowledgment form stating they have read or will read the content of the employee handbook and agree to abide by the Town's IT Policy. Five of the six users who accessed websites for personal and personal business use had signed an acknowledgment form. Officials could not provide an acknowledgment form for one user. We also reviewed acknowledgment forms for 14 additional users and determined that all of them had signed the acknowledgment form. When IT users

do not sign an acknowledgement form, the Town has less assurance that IT users are aware of the Town's IT Policy and its requirements, which increases the risk that the Town's IT systems and data could be exposed to loss or misuse due to high-risk Internet browsing.

While web filtering software can help mitigate instances of inappropriate and/or personal Internet browsing, periodically checking the Internet history would provide a more definitive review of activity to identify inappropriate and/or personal Internet browsing. Unauthorized internet browsing and personal use of Town computers increases the likelihood of exposing computer systems to malicious content that could compromise PPSI or the IT system.

In addition, officials did not provide IT security awareness training to help ensure employees understand IT security measures and their roles in safeguarding data from potential abuse or loss and protecting the Town's IT systems.

The failure to provide IT security training and raise awareness increases the risk that users will not understand their responsibilities, putting the data and IT systems at greater risk for unauthorized access, misuse, or abuse. As a result, the Town has an increased risk that it could lose important data and suffer a serious interruption in operations.

Recommendations

Town officials should:

1. Implement procedures to monitor employee Internet use and ensure compliance with the Town's IT Policy.
2. Ensure all IT users sign an acknowledgment form that indicates they are aware of and will comply with the Town's IT Policy.
3. Ensure IT security awareness training is periodically provided to all individuals who use Town IT resources.

Finding 2 – Town officials did not implement strong access controls.

Town officials have not implemented comprehensive procedures for managing and monitoring user access to the Town's network and computers. The Town IT Director configured and maintained the Town's IT environment, which included servers, desktops, network accounts and software applications.

We reviewed the Town's 228 enabled network user accounts and determined 11 user accounts were unneeded, or used seasonally, and should have been disabled when not in use. Specifically, we identified:

- Six accounts belonged to former Town employees who had left Town employment ranging from one week to three years.
- Three accounts were duplicate accounts for users created due to technical issues. Once the new accounts were created, 11 months to 16 months prior to our review, the technical issues were resolved and the old accounts were no longer needed.
- One account belonged to an employee who went out on medical leave about one year prior to our review.
- One account belonged to a seasonal employee whose access should have been disabled over two months prior to our review.

However, the IT Director did not disable these accounts, and they were still enabled.

Because the IT Director did not periodically review all user accounts, these unneeded accounts went unnoticed. When unneeded user accounts remain enabled, the Town has an increased risk that disgruntled employees or attackers could use these accounts as entry points to access PPSI and compromise IT resources.

Of particular risk are the accounts for former employees, which indicates the Town has inadequate account management and monitoring. Without adequate account management, the Town has an increased risk that attackers could successfully compromise its IT system. Also, because user accounts were not monitored, the Town has a greater risk that the Town would not notice whether the accounts had been compromised or used for malicious activities, which could give attackers more time and opportunities to access PPSI and compromise the Town's IT resources.

Recommendations

4. The IT Director should immediately disable the unneeded user accounts identified in this report.
5. Town officials should develop comprehensive written procedures for managing and monitoring user accounts that include periodically reviewing user access and disabling or changing accounts when access is no longer needed.

Finding 3 – The Board did not adopt an IT contingency plan or periodically test backups.

Although the IT Director had a draft IT contingency plan dated November 2022, the Board did not adopt it and the IT Director did not sign it to indicate he approved the draft plan. In addition, the draft IT contingency plan did not cover specific procedures to recover from an unexpected IT disruption. Furthermore, the draft IT contingency plan stated that it will be tested at least annually. However, the IT Director could not provide any documentation showing that the IT contingency plan was ever tested.

Computers connected to the network are backed up to the server daily, and the backups are stored both onsite and offsite. However, these backups were not periodically tested to ensure they will function as expected.

The IT Department receives daily alerts as to whether the daily backups were successful, had any errors or if they failed. The IT Director told us the IT Department did an initial restoration check on backups when the Town started using the current backup software in 2018. However, there is no schedule in place to restore or test backups periodically. He could not provide documentation for backup testing during our audit period.

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 disaster or other unexpected IT disruption. Also, by not testing backups, Town officials have limited assurance that important data will be available in the event of a loss. As a result, the Town has an increased risk that it could lose important data and suffer a serious interruption in operations.

Recommendations

The Board should:

6. Adopt an IT contingency plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed.

The IT Director should:

7. Establish procedures to ensure backups are routinely tested.

Appendix A: Profile, Criteria and Resources

Profile

The Town, located in Albany County, is governed by an elected five-member Board composed of the Supervisor and four Board members. The Village of Altamont is within the borders of the Town.

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 approximately 294 employees, 228 enabled network user accounts and 188 network computer accounts (servers, desktops and laptops).

Criteria – Information Technology

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 IT systems will remain safe.

The Town adopted an IT Policy specifying the acceptable and prohibited use of the Town's computer system. The Board should ensure officials monitor employees' computer use to ensure they comply with the Town's IT Policy. Monitoring for compliance with the IT Policy involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity. Automated mechanisms, such as web filtering software, may be used to perform this process and can help security professionals routinely assess computer security, perform investigations during and after an incident and even recognize an ongoing attempt of unauthorized access.

User accounts enable networks and computers to recognize specific users, grant appropriate user permissions and provide user accountability by associating user accounts with specific users. Town officials are responsible for restricting user access to only those applications, resources and data needed to complete job duties and responsibilities. This helps ensure IT data and assets are protected from unauthorized use and/or modifications. When employees leave Town employment or when user accounts are no longer needed, these user accounts should be disabled in a timely manner. Town officials should develop written procedures for granting, changing and removing user access and permissions to the overall networked computer system and to specific computers, applications and folders.

A 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, such as a flood or fire, that compromises the availability or integrity of town 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 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 help ensure backups will function as

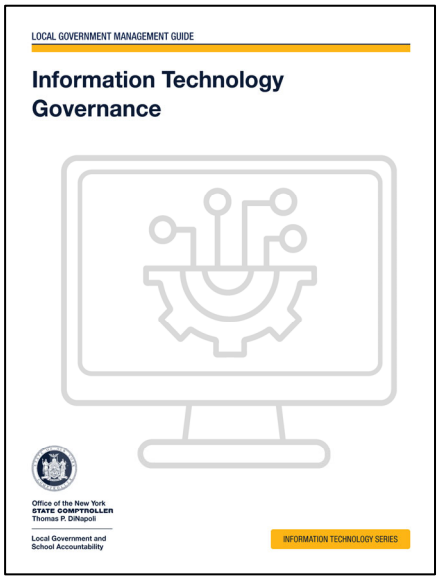
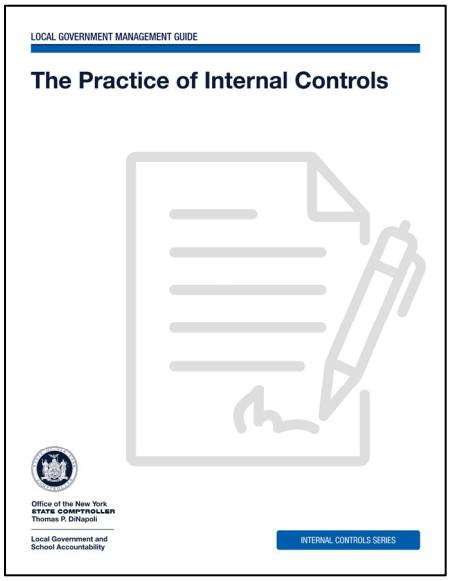
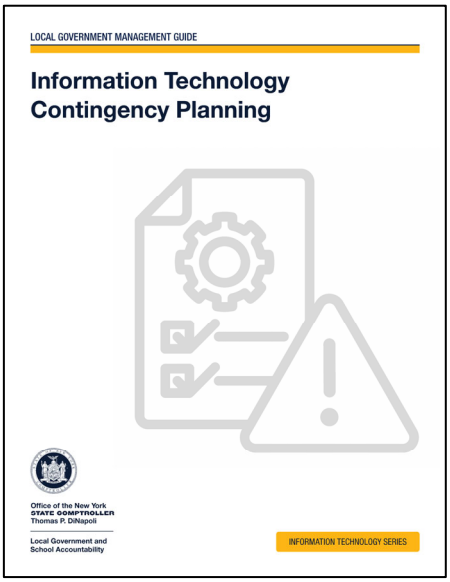
intended. To help minimize the risk of disruption, officials should have periodic IT security awareness training that explains common security threats and the proper rules of behavior for using the Internet and IT resources, systems and data. The training should communicate policies and procedures to all IT system users, so they understand IT security measures and their roles in safeguarding data and IT assets.

Town officials and employees are provided with an employee handbook which contains the Town's IT Policy. The policy states employee computer access is solely for Town employment duties and prohibits any computer use unrelated to the employee's employment. Furthermore, officials and employees need to sign an acknowledgment form stating they have read or will read the content of the employee handbook and agree to abide by the Town's IT Policy.

Additional IT Resources

Figure 2: 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

Information Technology Governance	*The Practice of Internal Controls*	*Information Technology Contingency Planning*
		
https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf	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/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 GUILDERLAND
Office of the Supervisor
Town Hall, Route 20
P.O. Box 339
Guilderland, NY 12084-0339
Phone: (518) 356-1980
Fax: (518) 356-5514

PETER G. BARBER
SUPERVISOR

JESSICA MONTGOMERY
SECRETARY

October 30, 2025

Via Email: Muni-GlensFalls@osc.ny.gov

Division of Local Government and School Accountability
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, NY 12081

Re: Information Technology Report of Examination (2025M-61)

Dear Madam or Sir:

We write in response to the Information Technology Report of Examination (2025M-61) ("Report") for the Town of Guilderland ("Town"). Upon behalf of the Town and its staff, we greatly appreciate the professionalism of your office's team during the audit process, and its very helpful recommendations and suggestions to improve the Town's practices. The following includes the Town's combined Collective Action Plan and Response.

Town's Response to Finding 1's Recommendations.

The Town is mindful of the importance of monitoring employee use of the internet and IT security awareness training. The IT Department deploys a very robust and integrated Firewall, Endpoint Protection Antivirus, and Managed Threat/Detection Response service that includes internet content filtering. The Report makes no reference to the IT Department's multiple compensating controls that enhance IT security.

See Note 1 Page 12

The IT Director also receives and reviews five distinct weekly web usage and bandwidth reports, makes timely inquires on questionable use of the internet by Town employees, and refers documented improper use of the internet to Human Resources. It is impossible to determine from these weekly reports whether the websites cited in the Report are used for Town purposes

or personal reasons. There is no known software that would determine whether a person is accessing a particular website for a proper Town use or personal use.

The Town's *Technology Policy & Procedure* sets forth provisions governing the proper use of Town computers and servers, including acceptable internet use. The improper use of the internet has been subject to disciplinary actions.

Corrective Action Plan for Finding 1's Recommendations.

- The Human Resources and IT Departments will update the *Technology Policy & Procedure* to allow for incidental personal use of computers similar to what is already allowed for Town-issued phones. The revised policy will be reviewed and adopted by the Town Board.

- The revised policy will again require written verification from each employee verifying that they have read and understand the updated internet use policy by signing an acknowledgement form.

- The IT Director has scheduled a Rapid Cyber Security Assessment with NYS Division of Homeland Security and Emergency Services in Spring 2026. The revised policy will again require employee security awareness training.

Town's Response to Finding 2's Recommendations.

The Town's *Cyber Incident Prevention Policy* requires the deactivation of retired employees accounts. The IT Department has implemented comprehensive procedures for managing and monitoring user access. There is a workflow in place with Human Resources for hiring and departing Town employees. The IT Department also requires periodic enhanced password changes [redacted] The Report does not mention these existing compensating controls for cyber incident prevention.

See Note 1 Page 12

Corrective Action Plan for Finding 2's Recommendations.

- During the audit, the IT Department immediately disabled all unneeded user accounts identified in the Report.

- The IT Department has written procedures with strict access controls for the Town's computers and networks, and will review the existing *Cyber Incident Prevention Policy,* and will again require periodic review of user access and the disabling or changing of accounts when access is no longer needed. It will also have the updated policy reviewed and adopted by the Town Board.

Town's Response to Finding 3's Recommendations.

The IT Department prepared and adheres to the *Information System Contingency Plan*, dated November 15, 2022, which call for activation, notification, recovery, and reconstitution of the information system. It does not appear that the Town Board formally adopted this policy. This policy was developed in accordance with Federal Information Processing Standards 199 (*Standards for Security Categorization of Federal Information and Information Systems*) and also requires periodic testing and regular backups. The Report does not note the existing compensating controls for protecting the Town's information system. The IT Director has also been discussing "sandbox" test full restorations and disaster recovery testing with the Town's failover servers [redacted]

See Note 1 Page 12

The IT Director is an active member of the Center for Internet Securit , Multi-State Information Sharin and Anal sis Center, and Water Information Sharin & Anal sis Center, and regularly meets State-wide IT Directors through the New York State Local Government Information Technolo Directors Association. IT staff also regularly attend seminars on best practices for contingency plans and incorporate them into its management of IT services.

Corrective Action Plan for Finding 3's Recommendations.

- The IT Department will review the existing *Information System Contingency Plan* for necessary updating, and distributed to all responsible parties. It will also have this contingency policy reviewed and adopted by the Town Board.

- As noted above, the Town has been working with Albany County's IT Disaster Recovery Center on conducting disaster recovery testing.

Very truly yours,

Peter G. Barber
Town Supervisor

Jeffery Gregory
Director, Information & Technology Services

cc: Town Board
Human Resources

Appendix C: OSC Comment on the Town's Response

Note 1

As a result of our planning and risk assessment process, we selected an objective that focused on officials' efforts to adequately secure and protect the Town's IT assets against unauthorized use, access and loss. Therefore, the audit report is focused on this program area. Our audit also examined the adequacy of other IT controls. Because of the sensitivity of this information, we communicated it confidentially to Town officials.

Appendix D: 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 and employees 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 existed, and Town employees received IT security awareness training.
- We used our professional judgement to select 14 computers based on the job titles and duties of the officials and employees who had access to these computers. The officials and employees using these computers had access to the Town's accounting software, online banking and police evidence. We ran a computerized audit script on the 14 computers on January 10, 2025, and reviewed the Internet history to determine whether employees accessed secured and appropriate websites.
- We reviewed signed acknowledgement forms on file at the Town for a sample of 20 users. We selected our sample based on the users' roles within the IT environment (14 users from various departments with different duties and system access) and the six users who accessed websites for personal and personal business use (as identified in our review of the Internet history).
- We reviewed the Town's employee handbook and IT Policy providing guidance to officials and employees on acceptable and prohibited computer use.
- We physically observed the Town's IT assets to determine whether the Town implemented appropriate physical security controls.
- We analyzed and assessed all 228 enabled network user accounts using a computerized audit script ran on January 10, 2025, and compared the network user accounts to the Town's employee master listing to determine whether there were any enabled user accounts assigned to former Town employees.

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.

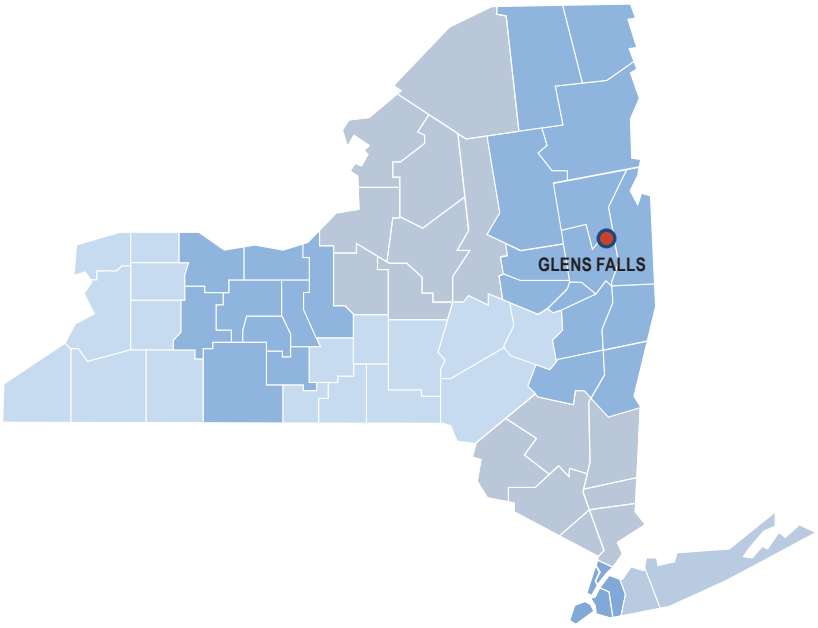
Contact

GLENS FALLS REGIONAL OFFICE – Gary G. Gifford, Chief of Municipal Audits

One Broad Street Plaza • Glens Falls, New York 12801-4396

Tel (518) 793-0057 • Fax (518) 793-5797 • Email: Muni-GlensFalls@osc.ny.gov

Serving: Albany, Clinton, Columbia, Essex, Franklin, Fulton, Greene, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington 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