



Steuben County

Safeguarding Computerized Data

2025M-96 | December 2025

Contents

Audit Results	1
Audit Summary	1
Safeguarding Computerized Data: Findings and Recommendations	3
Finding 1 – County officials did not inventory and classify computerized data.	3
Recommendations	4
Finding 2 – County officials did not update or test their IT contingency plan and backup procedures.	5
Recommendations	5
Finding 3 – County officials did not provide IT security awareness training.. . . .	6
Recommendations	7
Finding 4 – County officials did not properly manage network user accounts.. . . .	7
Recommendations	7
Appendix A: Profile, Criteria and Resources.	9
Appendix B: Response From County Officials.	12
Appendix C: Audit Methodology and Standards.	14

Audit Results

Steuben County



Audit Objective

Did Steuben County (County) officials limit and monitor access to and properly safeguard computerized data in the finance and personnel departments and County Clerk's office?

Audit Period

January 1, 2023 – July 31, 2025.

We expanded the scope of the audit to look at all network user accounts, permissions and security settings.

Understanding the Audit Area

County officials must safeguard computerized data in the finance and personnel departments and the County Clerk's office to help protect sensitive information, prevent fraud, comply with legal requirements and maintain public trust. Limiting and monitoring access is crucial to prevent unauthorized access by internal or external threats, which could lead to data breaches, financial theft, identity theft or other harmful consequences for individuals. Therefore, protecting computerized data is especially important as the number of instances of people with malicious intent trying to harm computer networks and/or gain unauthorized access to information using malware and other types of attacks continues to rise.

The Director of Information Technology (IT Director) serves as the Chief Information Officer (CIO) and oversees the IT department and computerized environment, including controls over computerized data. County officials¹ are responsible for designing and implementing policies and procedures to safeguard computerized data.

Audit Summary

County officials did not limit and monitor access to and properly safeguard computerized data used by employees in the finance and personnel departments and County Clerk's office. As a result, County officials cannot be assured that County-owned computerized data was secured and protected against unauthorized use, access and loss, and there is an increased risk that County officials could lose important data and suffer a serious interruption in operations.

¹ County officials include the Legislature, County Manager, County Clerk, Commissioner of Finance, Personnel Officer and IT Director.

Specifically, County officials did not:

- Inventory and classify computerized data, including personal, private or sensitive information (PPSI),²
- Ensure the security of County-owned data in the custody of third-party service providers,
- Update and test IT contingency planning and backup procedures,
- Provide periodic information security awareness training, and
- Ensure network user accounts were properly managed.

Sensitive IT control weaknesses were communicated confidentially to County officials.

The report includes 10 recommendations that, if implemented, will improve the internal controls over the County's IT system. County officials agreed with our recommendations and indicated they will take corrective action. County officials' responses are 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. Our methodology and standards are included in Appendix C.

The County Legislature (Legislature) 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 Legislature to make the CAP available for public review.

² 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.

Safeguarding Computerized Data: Findings and Recommendations

County officials and employees in the finance and personnel departments and County Clerk's office use County-owned IT computers, network and Internet resources; software; and third-party service provider software programs to perform day-to-day operations and collect, access and store computerized data. The various types of computerized data maintained by the finance and personnel departments, the County Clerk's office, the County IT department and third-party service providers include financial, personnel, legal and real property records that may contain PPSI.

A county's IT systems and the data they hold are valuable and need to be protected from unauthorized access and inappropriate and wasteful use or loss. County officials should establish IT policies and procedures that consider people, processes and technology. Inventorying and classifying computerized data helps identify where data resides and assigns a level of risk to various types of information to determine the level of security it needs. A comprehensive data classification policy defines PPSI, explains the county's reasons for collecting data, and describes specific procedures for the use, access to, storage and disposal of data. A comprehensive written IT contingency plan helps minimize the risk of data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster. An acceptable use policy describes appropriate and inappropriate use of IT systems and computerized data and the consequences of violating the policy. County officials should monitor compliance with these policies and develop and deliver periodic IT security awareness training. Furthermore, county officials should monitor the security of county-owned data maintained by third-party service providers and periodically review network user accounts to verify that they are necessary.

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

Finding 1 – County officials did not inventory and classify computerized data.

County officials³ did not complete an inventory or classification of computerized data, including PPSI. The County's information access policy states that the IT department manages and controls authorized access to computerized data owned by individual departments, and each department is responsible for authorizing access, creating, maintaining and disposing of the computerized data it uses. However, the information access policy does not establish procedures for inventorying and classifying computerized data or addressing County-owned computerized data maintained in third-party service providers' cloud applications. It should be noted that each of these concerns were also identified during a 2021 Health Insurance Portability and Accountability Act (HIPAA) risk assessment of the County's operations but were not addressed.

³ County officials include the County Clerk, Commissioner of Finance, Personnel Officer and IT Director.

According to the IT Director, data classification was not necessary because all data is secured at the HIPAA security standards⁴ for computerized data maintained by the IT department. In addition, individual department heads were responsible for notifying the IT department of who was authorized to access the computerized data. Employees in the finance and personnel departments and County Clerk's office were responsible for securing the data on their County-owned computers that was not maintained by the IT department. However, no one in the finance and personnel departments or County Clerk's office maintained an inventory of computerized data maintained on their staff's County-owned computers by the IT department or third-party service providers, and there were no procedures for securing and disposing of the computerized data in their possession.

In addition, County officials did not ensure third-party service providers secured County-owned data. County officials did not have a service level agreement (SLA) for one of the two third-party service providers that maintained custody of County-owned data for use by the finance and personnel departments. County officials also did not perform a review of the security controls used by the third-party service providers for County-owned data in their custody or request a service organization control (SOC) report⁵ as outlined in the one available SLA.

Because County officials do not know what computerized data they have or where it is located, they cannot ensure it is safeguarded. Unless County officials classify the computerized data they maintain, set appropriate security levels for PPSI and prepare and update data classification and inventory on an ongoing basis, there is an increased risk that PPSI, such as employee Social Security numbers, vendor employer identification numbers and medical information, could be inadvertently exposed, misused or altered by unauthorized users. Furthermore, lack of information about the types and extent of computerized data the finance and personnel departments, the County Clerk's office and third-party service providers maintain and where PPSI resides can hamper efforts to properly notify affected parties in the event of a breach or to restore operations after a disruption of services.

Recommendations

County officials should:

1. Complete an inventory and classify computerized data according to its type and sensitivity and update it on an ongoing basis.
2. Develop an SLA with each third-party service provider that addresses the safeguarding of County-owned data in their custody.
3. Annually require and review SOC reports from the third-party service providers.

⁴ "HIPAA security standards comprise a defined set of administrative, physical and technical safeguards that include implementing security procedures, providing awareness training, developing a contingency plan, properly handling electronic media (e.g., removable storage devices) and permitting access to authorized users only."

⁵ A SOC report provides valuable information from an independent reviewer about the third-party service provider's infrastructure, controls, risks and the effectiveness of the controls in place

Finding 2 – County officials did not update or test their IT contingency plan and backup procedures.

Although County officials⁶ and IT department staff developed IT Contingency Plan and Backup procedures, the plan was outdated, not disseminated to appropriate County officials and employees or regularly reviewed and tested. County officials created the plan in May 2017 and included procedures related to data backup, disaster recovery, emergency mode operation, testing and revising, and applications and data criticality analysis. In addition, the list of IT team members charged with implementing the plan and their personal contact information was outdated because it contained former employees and incorrect contact information.

The IT Director stated that the plan would not be used in the event of an emergency because it is outdated and that the IT department does not have the staff available to update it. He also stated that the IT department regularly performs full server backups instead of just the computerized data. However, backups were only restored as needed and not periodically tested.

Without an up-to-date contingency plan, County officials have less assurance that, in the event of a disruption or disaster such as a ransomware attack, inadvertent employee action or power outage, employees and other responsible parties would be able to react quickly and effectively to help resume, restore, repair and/or rebuild critical IT systems, applications or data in a timely manner. Depending on the severity of an incident, County officials may need to expend significant time and financial resources to resume County operations.

Furthermore, responsible parties may not be aware of their roles, complicating the County's ability to recover from an incident. Finally, by not periodically testing backups, County officials cannot ensure they will function as expected. As a result, the County has an increased risk that it could lose important computerized data and suffer a serious interruption in operations that depend on its computerized environment, such as not being able to process checks to pay vendors or employees.

Recommendations

County officials should:

4. Update their IT Contingency Plan and Backup procedures and ensure they are distributed to all responsible parties.
5. Periodically test full-server backups.

⁶ County officials include the County Manager, Deputy County Manager and IT Director.

Finding 3 – County officials did not provide IT security awareness training.

County officials did not provide staff with IT security awareness training to help ensure they understand IT security measures and their roles in safeguarding computerized data and other IT assets. Personnel department staff provided staff at their new employee orientation with the computer usage policy and an information sheet on the County's internal bulletin board that included articles on IT topics. However, County officials in the finance and personnel department and County Clerk's office did not provide their department's staff with annual IT security awareness training as required to ensure they understand IT security measures and their roles in safeguarding computerized data and other IT assets. The Commissioner of Finance, Deputy Personnel Officer and Deputy County Clerk stated that they were unaware of the County's IT policy requirement to do so. In addition, the County's internal bulletin board for information security tips and current threats does not send notifications to employees when new information is posted and has not been updated since early 2023 by IT department staff.

Although IT department staff conduct an annual phishing test,⁷ users that fail the phishing test are not required to take additional training. According to the results from the phishing test conducted in January 2025, 210 of the 667 recipients (32 percent) failed the phishing test.

Because IT security awareness training was not provided, we reviewed the Internet history on nine computers within the finance and personnel departments and County Clerk's office. We determined that 13 of the 15 users on the nine computers reviewed had 85,916 website visits.

- The large amount of Internet history occurred because employees and County officials did not delete their Internet history after each Internet browsing session. For example, one user's Internet history dated back to April 2023, while others included three to six months of Internet history.
- All eight computers assigned to individual users had personal Internet use and four of the eight users had more than incidental personal use, which was not in compliance with the County's IT policy. The personal use related to visits to newspapers, travel, entertainment, non-County email, vacation planning, healthcare and shopping websites.
- Website visits by five users in the finance department and the County Clerk's office totaled 2,928 of the 85,916 website visits and included possible PPSI exposures.

Had employees and County officials been provided with adequate IT security awareness training, they may have recognized and notified the IT department of the possible PPSI exposure, or been aware to routinely delete their Internet history after each Internet browsing session to ensure any PPSI exposed could not be viewed by unauthorized individuals. Group policy configurations could be used to automate the deletion of browser histories on browser exit. Without periodic, comprehensive IT security

⁷ A type of security awareness program that simulates, for training purposes, a cybercriminal posing as a legitimate party in an attempt to get victims to engage with malicious content or links, to share personal or sensitive information, or infect computers with malware such as ransomware.

awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, County-owned computerized data and PPSI could be at greater risk for unauthorized access, misuse or loss.

Recommendations

6. County officials should provide periodic IT security awareness training to all users of County-owned IT resources that includes the importance of appropriate computer use and monitor compliance with the County's computer use policy.
7. IT department staff should communicate, such as through regular updates on the County's internal bulletin board or County-wide email messages, to all users of County IT assets the IT security measures and their roles in safeguarding computerized data and other IT assets.

Finding 4 – County officials did not properly manage network user accounts.

County officials did not properly manage network user accounts. Although there is a policy that addresses granting, changing and revoking access to the network and software applications, it does not require periodic reviews by IT department staff or the Network Administrator. Furthermore, change forms were not always completed for all requests. As a result, we identified 364 out of 1,345 accounts that were not used in the previous six months and 49 of them were unneeded network user accounts, including former employees and unused and contractor accounts, that were not disabled by the IT department. When network user accounts are not used or monitored, IT department staff cannot detect compromised accounts in a timely manner.

Unneeded network user accounts are additional entry points into a network and, if accessed by an attacker, could severely disrupt County operations or be used to inappropriately access the County's network to view and/or remove PPSI, make unauthorized changes to County records or deny legitimate access to the County's network and records.

Recommendations

8. County officials should complete change forms for granting, changing and revoking network user accounts.

-
9. The Network Administrator or IT department staff should disable network user accounts of employees and contractors as soon as they leave County employment or service and disable other unneeded network user accounts.
 10. The Network Administrator should conduct periodic reviews of network user accounts.

Appendix A: Profile, Criteria and Resources

Profile

The County has 1,288 employees, which includes 17 IT department, 10 County Clerk, eight finance department and seven personnel department employees. During our audit period, there were 1,345 network user accounts enabled with 1,353 devices.

The County covers approximately 1,400 square miles, has approximately 94,000 residents and encompasses 32 towns, 14 villages and two cities. The County is governed by the Legislature, which includes 17 elected members, one of whom serves as the Chair. The County Manager is appointed by the Legislature and serves as the County's chief executive officer responsible for the day-to-day operations along with other County officials. The IT Director serves as the CIO and oversees the County's IT environment, including controls over computerized data. The CIO is assisted by 17 employees, including the Network Administrator who is responsible for managing and maintaining the County's computer networks. The County relies on its IT system to perform a variety of tasks, including: providing Internet access and email communication, storing data, recording financial transactions and reporting to State and federal agencies.

The Commissioner of Finance is appointed by the Legislature and serves as the chief fiscal officer. The finance department consists of eight employees that collect delinquent property taxes, manage and invest County funds, conduct banking and financial transactions, administer the computerized accounting and various financial reporting systems, process payroll and benefits for almost 1,300 employees and County officials, and make vendor payments.

The Personnel Officer is appointed by the Legislature and oversees six employees in the personnel department. Employees in the personnel department develop and administer a comprehensive personnel management system, including employee staffing, training, benefits administration and wages.

The County Clerk is an elected official responsible for recording, filing and preserving a variety of records and processing and issuing a variety of documents. There are 10 employees in the County Clerk's office that process these records and documents. The County Clerk also serves as Clerk of the State Supreme and County Courts and is responsible for filing and maintaining court files.

Criteria – Safeguarding Computerized Data

A county's IT system and the computerized data it holds are valuable resources that need to be protected from unauthorized, inappropriate and wasteful use. Even small disruptions in IT systems can potentially require extensive time and effort to evaluate, repair and/or rebuild.

Data classification is a necessary part of information security management. A comprehensive PPSI classification policy defines PPSI, explains the county's reasons for collecting PPSI, and describes specific procedures for the use, access to, storage and disposal of PPSI involved in normal business activities. The policy should also include data classification requirements. All information, whether

in printed or electronic form, should be classified and labeled in a consistent manner to ensure data confidentiality, integrity and availability. The data classification process assigns a level of risk to various types of information, which helps county officials make appropriate decisions about the level of security the data requires. Therefore, it is important that county officials classify information in a consistent manner to determine the appropriate level of security for each type of data.

County officials also should conduct an inventory of computerized data, including PPSI, stored on all their electronic equipment to account for the confidential data maintained. County officials should update the classification and inventory list on an ongoing basis, as appropriate, to reflect any changes. In the event of a data breach, the proper classification and inventorying of PPSI allows county officials to determine the extent of unauthorized access and take appropriate action.

In addition, county officials should have a separate written SLA between the county and its third-party service providers that identifies the county's needs and expectations and specifies the level of services to be provided. An SLA establishes 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 a written contract and SLA with the third-party service providers will allow county officials to monitor the third-party service provider's work to ensure that the county is receiving all contracted services.

In addition, county officials should develop and adopt a comprehensive written IT contingency plan to help minimize the risk of data loss or suffering a serious interruption of service in the event of an unexpected IT disruption or disaster. A disruptive event could include a power outage, software failure caused by a virus or other type of malicious software, equipment destruction, inadvertent employee action or a natural disaster, such as a flood or fire, that compromises the availability or integrity of county services, including the IT system and data.

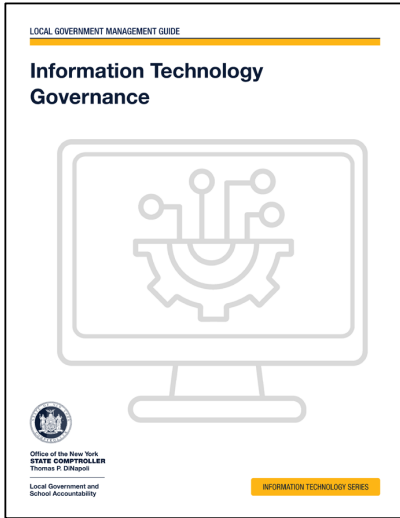
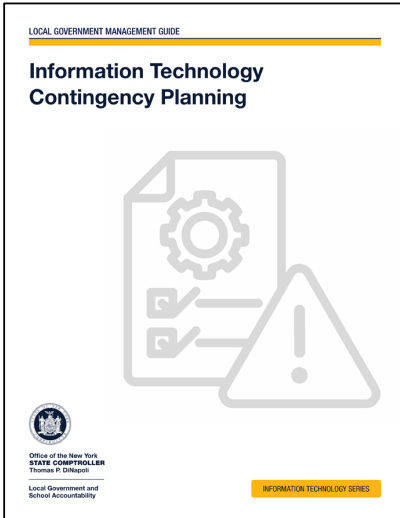
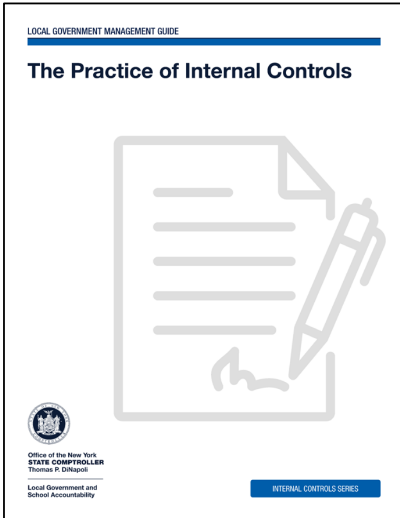
Typically, IT contingency planning involves analyzing business processes and continuity needs, focusing on sustaining critical functions and identifying roles of key individuals and necessary precautions needed to maintain or quickly resume operations. The plan should be periodically tested and updated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

Network user accounts provide access to network resources and should be actively managed to minimize the risk of unauthorized use, access and loss. Network user accounts are potential entry points for attackers because, if compromised, they could be used to inappropriately access and view PPSI on the network, make unauthorized changes to county records or deny legitimate access to network resources. To actively manage network user accounts, when network user accounts are no longer needed, they should be disabled in a timely manner. Additionally, county officials should maintain

a list of authorized network user accounts and routinely review enabled network user accounts to ensure they are still needed and disable unneeded network user accounts.

Additional Safeguarding Computerized Data Resources

Figure 1: OSC Publications

OSC Local Government Management Guides available on our website to help officials understand and perform their responsibilities.		
Information Technology Governance	Information Technology Contingency Planning	The Practice of Internal Controls
		
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	https://www.osc.ny.gov/files/local-government/publications/pdf/the-practice-of-internal-controls.pdf

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

Appendix B: Response From County Officials



STEUBEN COUNTY LEGISLATURE

*Kelly H. Fitzpatrick, Chair
District 3*

Ms. Stephanie Howes
Chief of Municipal Audits
Division of Local Government and School Accountability
Office of the State Comptroller

Dear Ms. Howes,

On behalf of Steuben County, I write in response to the IT Audit of Steuben County. We appreciate the diligence of staff of the Office of the State Comptroller during the audit process and the findings and recommendations shared with us. Below, please find our responses to each of the four findings from this audit.

Finding 1 – County officials did not inventory and classify computerized data.

County officials acknowledge the finding regarding the absence of a formal, countywide inventory and classification framework for managed data. While individual departments maintain their own operational data repositories, we recognize that the County has not yet implemented a standardized classification model or centralized documentation to ensure consistent data handling, access controls, and protection of sensitive information.

Although the County currently applies access controls and classifications necessary to meet HIPAA requirements, we understand the need for a more comprehensive and granular approach aligned with a recognized cybersecurity framework such as NIST. As part of our broader effort to strengthen Steuben County's security posture and align with the NIST 2.0 framework, the County will be developing formal documentation and implementing a standardized data classification structure to ensure consistent, secure, and compliant management of all computerized data.

Finding 2 – County officials did not update or test their IT contingency plan and backup procedures.

County officials acknowledge the finding related to the lack of updates and formal testing of the County's IT contingency plan and backup procedures. While various backup processes and recovery capabilities are currently in place, we recognize that the existing documentation and testing schedule do not fully meet best practices or audit expectations. Maintaining a current, validated contingency plan is critical to ensuring continuity of government operations and safeguarding County systems against disruptions, data loss, or cybersecurity incidents.

Finding 3 – County officials did not provide IT security awareness training

County officials acknowledge the finding related to the lack of formal, documented security awareness training for County employees. While informal guidance and ad-hoc communication have been provided in the past, we recognize the need for a structured, trackable, and policy-driven program to ensure all employees understand their cybersecurity responsibilities and remain compliant with best practices, state requirements, and regulatory standards.

Steuben County is currently implementing an annual cybersecurity training requirement through [REDACTED] the platform our Personnel Department is adopting to standardize all mandatory yearly trainings and maintain centralized training records. This initiative will support consistent employee education, improved accountability, and enhanced overall security posture.

Finding 4 – County officials did not properly manage network user accounts.

County officials acknowledge the finding related to the management and review of network user accounts. While policies exist that address the creation, modification, and revocation of access, we recognize that the current procedures do not require periodic review by IT staff and that account change forms were not

*Steuben County Office Building, 3 East Pulteney Square, Bath, New York 14810-1557
Telephone (607) 664-2243; Fax (607) 664-2282*

consistently completed or retained. The County also acknowledges the existence of inactive and unnecessary accounts, including accounts belonging to former employees and contractors, which were not disabled in a timely manner. Strengthening these procedures is critical to maintaining proper access controls, reducing cybersecurity risk, and ensuring compliance with best practices.

Thank you again for your efforts and collaboration.

Respectfully,

Kelly H. Fitzpatrick
Chair, Steuben County Legislature

*Steuben County Office Building, 3 East Pulteney Square, Bath, New York 14810-1557
Telephone (607) 664-2243; Fax (607) 664-2282*

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 County officials and staff and reviewed relevant IT policies and procedures, the IT contingency plan, and security controls in place to gain an understanding of the County's IT environment and the IT environment within the finance and personnel departments and County Clerk's office.
- We ran computerized audit scripts on December 16, 2024 on the County's domain controller to determine information pertaining to network user accounts, access rights and controls. We compared the 1,345 enabled network user accounts to the active employee list to identify potentially unneeded accounts. We followed up with the IT Director, Personnel Director and Deputy Personnel Director and individual department heads to determine whether the accounts were needed or should have been disabled.
- We ran computerized audit scripts on December 19, 2024 on nine judgmentally selected computers used by staff in the finance and personnel department and County Clerk's office with access to PPSI.
 - We analyzed the results generated by the script to obtain information about the computers' local user accounts, including their permissions and security settings, to determine whether they were necessary and appropriate.
 - We exported the Internet history files from the nine computers, which included 15 users and examined the data for indications of personal Internet use, based on the County's IT policy guidelines.
- We obtained and reviewed the results of the County IT department's phishing test conducted in January 2025.
- On March 7, 2025, we observed the County's internal bulletin board and noted the date of the last update and the types of IT security information provided to County officials and staff.
- We obtained and reviewed four new employee orientation checklist forms from the personnel department to determine whether staff hired during our audit period received and acknowledged receipt of the computer use policy and information about the internal bulletin board.
- We requested the SLAs for the two cloud-based third-party service providers and reviewed the one SLA provided to determine whether County-owned data in their custody was safeguarded.

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 County 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.

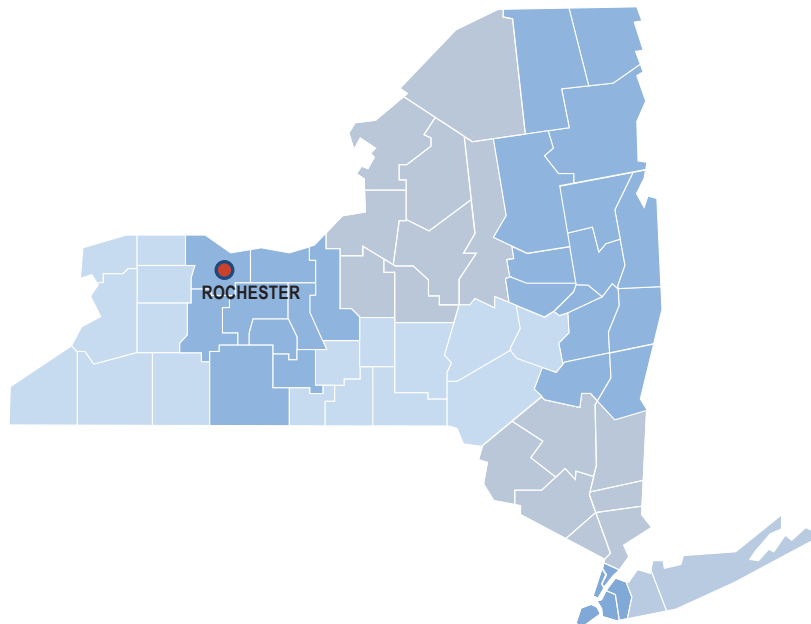
Contact

ROCHESTER REGIONAL OFFICE – Stephanie Howes, Chief of Municipal Audits

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates 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