

New York State Comptroller
THOMAS P. DiNAPOLI

City of Oneonta

Cybersecurity

October 2026 | 2026M-42

Prepared by the Division of Local Government and School Accountability

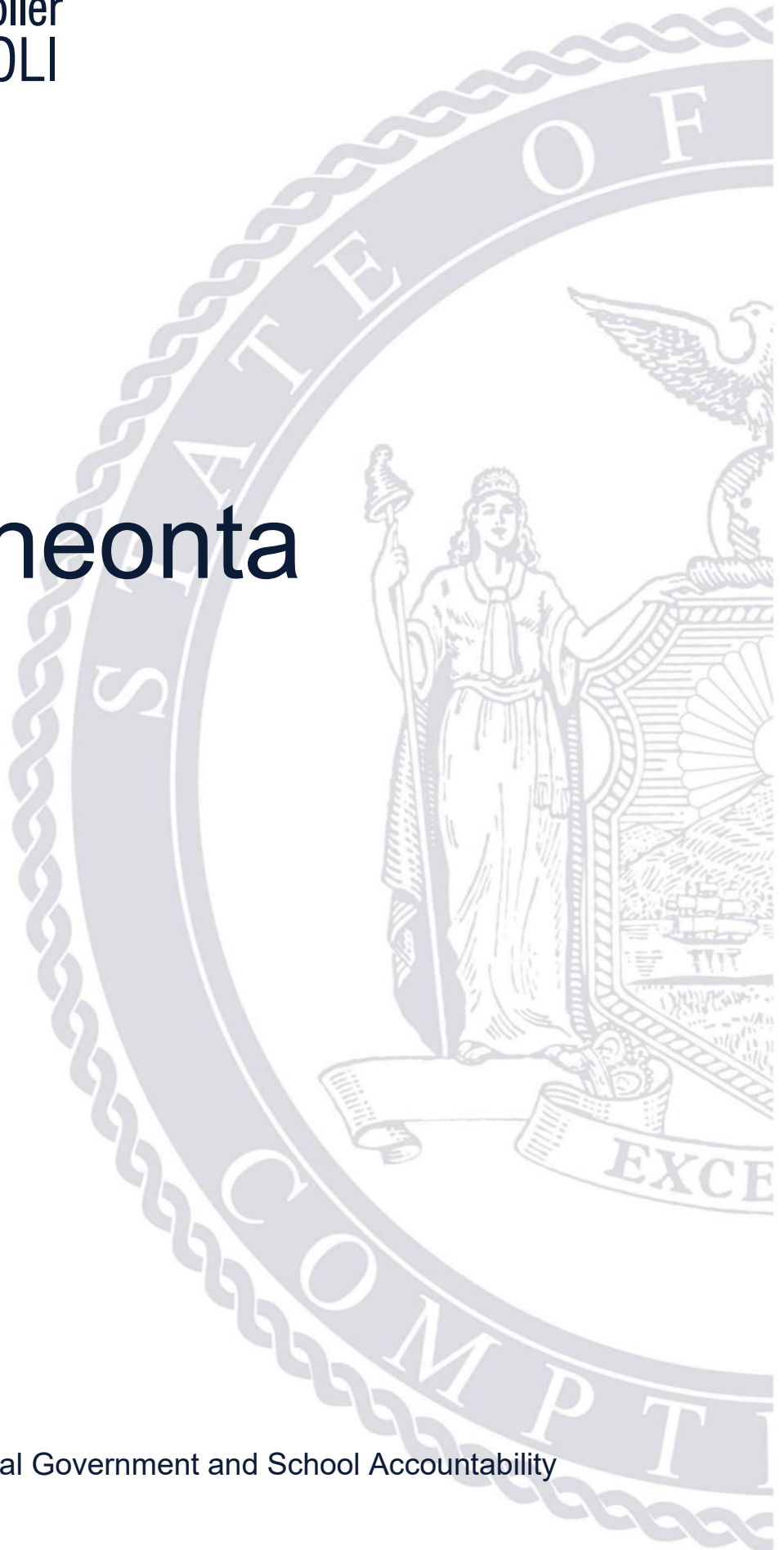


Table of Contents

Audit Results	1
Cybersecurity: Findings and Recommendations	3
Finding 1 – City officials did not ensure that employees completed cybersecurity awareness training.	4
Recommendation	4
Finding 2 – City officials did not ensure that cybersecurity risk assessment results were adequately documented.	4
Recommendation	5
Finding 3 – The Council and City officials did not adopt, review or enforce cybersecurity policies, resulting in a lack of oversight.	5
Recommendations	6
Finding 4 – The Council and City officials did not communicate cybersecurity policies or clearly document cybersecurity roles and responsibilities.	6
Recommendations	7
Appendix A: Profile, Criteria and Resources	8
Profile	8
Criteria	8
Additional Resources	9
Appendix B: Response From City Officials	10
Appendix C: OSC Comments on the City’s Response	14
Appendix D: Audit Methodology and Standards	15

Audit Results

City of Oneonta

Audit Objective

Did City of Oneonta (City) officials provide adequate governance to safeguard information technology (IT) assets from cybersecurity threats?

Audit Period

January 1, 2024 – November 7, 2025

Understanding the Audit Area

City 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.

During the audit period, the City paid an external IT service provider \$222,752 to perform various IT services, including hardware maintenance and repair, security services and other IT support services. The City had 188 employees and 106 computers as of July 2025.

Audit Summary

City officials did not provide adequate governance to safeguard IT assets from cybersecurity threats. While the City’s third-party IT vendor created several cybersecurity policies, standards and guidelines, the City’s Common Council (Council) did not formally adopt the policies and City officials did not review, enforce or monitor employee compliance with the policies. In addition, officials did not communicate the policies to City employees in a timely manner, and they did not clearly document cybersecurity roles and responsibilities in City employees’ job descriptions. As a result, policy violations occurred, including officials not documenting risk assessment activities and employees not completing cybersecurity awareness training within 30 days of hire.

Without effective cybersecurity governance, including Council-adopted and enforced policies, clearly documented roles and responsibilities, risk assessment documentation and cybersecurity awareness training, the City 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 exfiltration or corruption by malicious actors, and increased remediation and recovery costs. In addition, unclear job descriptions may lead to decreased efficiency of cybersecurity efforts, overreliance on individuals and inadequate segregation of duties. Cybersecurity governance weaknesses may also lead to ineffective cybersecurity risk management and inefficient incident response, which could potentially result in unauthorized access to City IT assets and data.

Sensitive IT control weaknesses were communicated confidentially to officials.

The report includes seven recommendations that, if implemented, will improve the City’s cybersecurity governance, improve accountability for cybersecurity responsibilities, enhance compliance with adopted policies and reduce the risk of unauthorized access, data loss and disruption of critical IT services. City officials disagreed with certain aspects of our findings, and their response is included in Appendix B. Our comments on the City’s response 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.

This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the Office of the New York State Comptroller's (OSC's) authority as set forth in Article 3 of the New York State General Municipal Law (GML). The audit's methodology and standards are included in Appendix D.

The Council 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 OSC within 90 days, pursuant to Section 35 of GML. For more information on preparing and filing the CAP, please refer to the OSC brochure, *Responding to an OSC Audit Report*, which was provided with the draft audit report. The Council is encouraged to make the CAP available for public review in the City Clerk's (Clerk's) office.

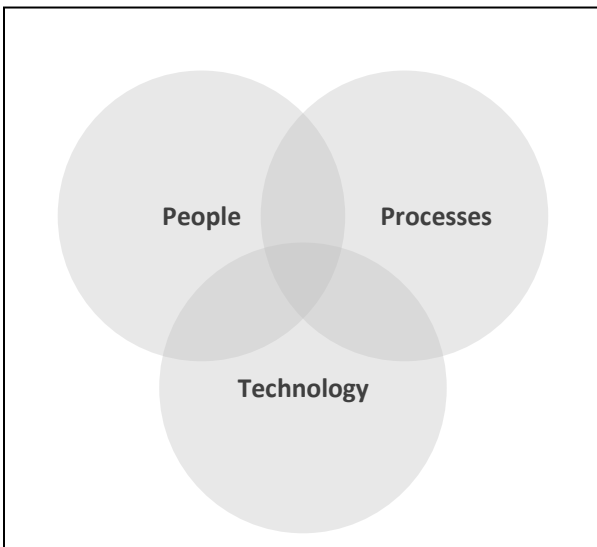
Cybersecurity: Findings and Recommendations

Cybersecurity threats are an ever-present risk to organizations, and the risk to IT is on par with economic, legal, operational, financial, political and safety risks. Managing these risks, and the threats from which they stem, is one part of an overall risk management program. A successful risk management program requires effective governance and communication among a city's common council and all executive and department officials to enable informed risk management decisions. Many cybersecurity vulnerabilities can be mitigated with no or minimal additional cost. It is imperative that city officials partner together to address cybersecurity risks and help protect IT assets against prevalent and emerging threats.

City officials should treat cybersecurity risks with the same seriousness and precaution as they would traditional safety risks. Cybersecurity risk management includes identifying and mitigating risks, remediating vulnerabilities and planning for contingencies. This requires an investment of time and resources, and a collaborative work environment among city officials and others responsible to help manage and secure a city's IT assets.

A city's IT assets and the data they support are valuable and need to be protected from unauthorized access, inappropriate use and loss. Cybersecurity policies should establish requirements for baseline security measures that should be implemented to help ensure a city's IT assets are safeguarded. A common council should adopt cybersecurity policies that help safeguard IT assets from cybersecurity threats and that consider the unique interactions among people, processes, and technology (Figure 1). Policies are the constitution of governance, and without formally adopted policies, a common council cannot provide effective oversight. Effective policies align with the city's mission and assist with providing adequate governance.

Figure 1 – The Interactions Among People, Processes and Technology



A common council and city officials should clearly communicate cybersecurity policies to employees and, if applicable, key personnel to help ensure understanding and compliance. When policies are not communicated clearly, employees may be unaware when they violate policies, resulting in inadvertent IT asset misuse or insecure handling. Clearly communicating policies is especially important when policy violations may result in cybersecurity compromises or data breaches. For example, employees who violate an acceptable use policy (AUP) may accidentally respond to phishing attempts or unknowingly download malicious software. Additionally, the common council should ensure that city officials develop and implement procedures to monitor and appropriately document policy compliance.

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

Finding 1 – City officials did not ensure that employees completed cybersecurity awareness training.

We determined that 11 out of 15 employees reviewed² (73 percent) did not complete cybersecurity awareness training within 30 days of hire and annually thereafter, as required by the City's 2022 and 2025 information security policies. The 11 employees had hire dates ranging from 2007 to 2025. Furthermore, two of the four employees (50 percent) who completed cybersecurity awareness training within 30 days of hire did not complete the training annually thereafter. Cybersecurity awareness training helps to educate employees about cybersecurity best practices and risks, and their responsibilities for helping to safeguard IT assets. Seven Council Members and the Clerk, City Administrator (Administrator) and Director of Finance (Director) were not aware the employees did not complete the required training. Furthermore, City officials did not track which employees completed the training to help monitor policy compliance (see Finding 3).

Cybersecurity awareness training is essential to convey expectations for baseline security, inform employees on how to respond to potential cybersecurity incidents, and address any new technologies, threats or other changes impacting the City's IT assets or safeguards. Cybersecurity awareness training also helps properly align employees' use and handling of IT assets with the City's mission and acceptable use policy. Without providing cybersecurity training and raising awareness about cyber threats to IT assets, there is an increased risk that employees will not understand their responsibilities related to IT asset safeguards and cybersecurity, which could result in inadvertent data leaks, increased susceptibility to phishing attacks and delayed cyberattack response. 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 City employees.

Recommendation

1. City officials should ensure that all employees complete cybersecurity awareness training within 30 days of hire in accordance with City policy and at least annually thereafter as required.

Finding 2 – City officials did not ensure that cybersecurity risk assessment results were adequately documented.

City officials worked with the IT vendor to perform cybersecurity risk assessment activities, such as vulnerability management. However, officials did not maintain adequate documentation of the risks identified during assessments and the remediation steps planned or completed, as required by the City's 2022 and 2025 information security policies. Assessing risks for IT systems is critical for identifying, tracking and mitigating threats to the City's cybersecurity and IT asset safeguards. Because City officials did not review, monitor or communicate the City's IT policies to employees (see Finding 3), the Administrator was unaware that risk assessments and applicable documentation were required.

Without risk assessment documentation, City officials may have difficulties routinely and consistently tracking risks and their associated mitigation needs or efforts. Such difficulties could lead to cybersecurity risks remaining unaddressed and officials relying on inaccurate or incomplete risk information, diminishing their ability to make informed cybersecurity governance decisions.

² Refer to Appendix C for information on our sampling methodology.

Recommendation

2. City officials should conduct, maintain and review complete, accurate and up-to-date documentation of IT system risk assessment results as required by their City policy.

Finding 3 – The Council and City officials did not adopt, review or enforce cybersecurity policies, resulting in a lack of oversight.

The City paid an annual service fee to the IT vendor totaling \$59,400. The IT vendor services included developing, updating and maintaining the City's IT policies and standards.³ While the IT vendor provided several policies, standards and guidelines to the City in 2022 and 2025, key City officials did not review them, and the Council did not formally adopt them as City policies. Instead, the Clerk, who did not have IT oversight as part of their documented roles and responsibilities and was not formally assigned the responsibility by the Council, was working as a liaison with the IT vendor to facilitate the provision of services.

Policies are a foundational component for establishing cybersecurity governance so that City IT asset use and safeguards can be clearly aligned with the City's mission to provide services to residents. The Council and City officials should review the policies provided by the IT vendor to ensure the City receives the services for which it paid. In addition, reviewing these policies ensures that they are accurate representations of the Council's expectations and that they clearly define any requirements the Council sets forth to help safeguard IT assets.

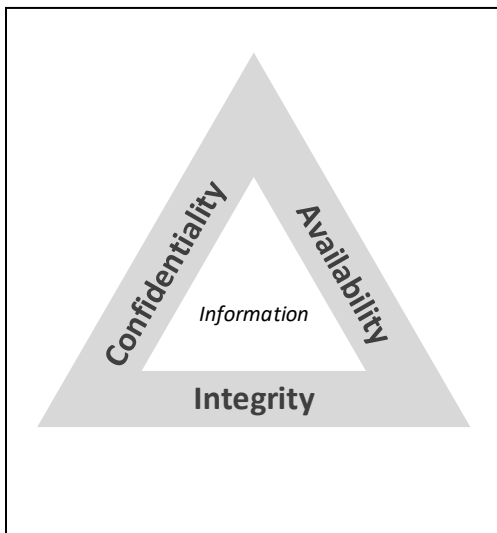
Four Council Members told us they agreed that the Council should adopt cybersecurity policies and three Council Members told us the Council should not adopt the vendor-provided policies because they did not want to interfere in the City's day-to-day operations. However, formally adopting policies enables the Council to establish the policies with the Council's authority and demonstrate an expectation of compliance to City officials and employees. Because the Council did not adopt policies, some City departments were unclear on which policies they should follow. For example, officials in the City's human resources department were unaware of the 2022 and 2025 vendor-provided updates to the AUP and were providing newly hired employees with the Council-adopted 2018 AUP.

In addition, the 2022 City policies required annual reviews to ensure relevancy. Annual policy reviews help ensure that policies reflect organizational changes, such as IT infrastructure or personnel changes. Because the Council and key City officials, such as the Administrator, did not review the 2022 and 2025 policies provided by the IT vendor, several policies contained inaccurate or irrelevant information. For example, one 2025 policy referenced a City IT manager position that did not exist, and other 2022 policies and standards stated that the City Mayor (Mayor) can grant policy exceptions although the Mayor was not granted this authority in the City's charter.

Finally, City officials did not monitor or enforce compliance with several key cybersecurity policies, including both the 2022 and 2025 information security and information classification policies. As noted in Finding 1, while the 2022 and 2025 information security policies required employees to complete cybersecurity awareness training within 30 days of hire, officials did not ensure all employees completed the required training. In addition, the information classification policies required all City information to be classified and appropriately documented based on confidentiality, integrity and availability metrics (Figure 2). While City officials established controls that used the required classifications, they could not provide us with the documentation required to explain the classifications' determinations and reasonings because the Administrator and other officials were unaware of the policy requirement and did not ensure that the requirements were being met.

³ Standards describe the defined requirements regarding processes, actions and configurations and are used to enforce policies, which are high-level statements of a local government's intent.

Figure 2 – The “Confidentiality – Integrity – Availability” (CIA) Information Classification Triad



Enforcing and monitoring policy compliance helps ensure IT asset use and safeguards align with the City’s mission and services. Without proper monitoring, policy violations can occur and increase the risk of a successful cyberattack, which could lead to IT system downtime and disruption, the inability to provide services reliant on IT assets, data exfiltration or corruption by malicious actors, and increased remediation and recovery costs.

Recommendations

The Council should:

3. Review and formally adopt cybersecurity policies provided by the IT vendor or developed by City officials.

City officials should:

4. Review and update, as needed, cybersecurity policies, standards and guidelines when provided by the IT vendor and at least annually thereafter.
5. Routinely monitor and enforce policy compliance and ensure policy violations are detected, addressed and documented in a timely manner.

Finding 4 – The Council and City officials did not communicate cybersecurity policies or clearly document cybersecurity roles and responsibilities.

The Council and City officials did not ensure that several key cybersecurity policies, including both the 2022 and 2025 versions of the AUP and the 2025 cyber incident response plan, were communicated to all relevant employees, or ensure that employees’ job descriptions included clearly defined responsibilities for their designated cybersecurity roles. The Administrator and four Council Members were not aware of what was written in the 2022 and 2025 policies and could not communicate the information to personnel.

New employees were required to sign the 2022 and 2025 AUP to indicate their understanding and agreement to the policy’s requirements. However, because the Council did not adopt and communicate policy updates, officials in the human resources department were unaware of policy updates to the AUP and provided new

hires with the previously Council-adopted 2018 AUP even though the IT vendor provided the Clerk the updated 2022 and 2025 acceptable use policies (see Finding 3).

The Council and City officials also did not notify employees designated in the City's 2022 and 2025 cyber incident response plan that they were responsible for specific roles in responding to cyber incidents. Similarly, the Chief of Police told us he believed the department would be notified of any cyber incident involving a criminal element. While the 2022 cyber incident response plan included the City law enforcement's contact information, the 2025 cyber incident response plan stated that law enforcement's response time and competency in responding to an incident would vary and that there may be a loss of reputation if certain incidents reached the public. This wording in the 2025 cyber incident response plan could create a difference in cyber incident reporting among the City's staff. The 2022 cyber incident response plan did not contain specific consideration for the City's departments' needs in a cyber incident, or how the City's departments would be communicated with during an incident.

Furthermore, technology and threats frequently change, creating the need for officials to periodically revisit IT and cybersecurity roles and responsibilities. However, City employees' IT roles and responsibilities were last updated in 2020. As a result, City employees' roles and responsibilities were not clearly and accurately defined in their documented job descriptions.

For example, the Clerk's responsibilities included serving as the primary IT contact for City employees, monitoring IT vendor services, overseeing IT-related projects and performing user account reviews. However, the Clerk's documented job responsibilities only included "additional IT, website, and related technology duties," which did not match the responsibilities the Clerk was performing. Similarly, while the Director's job description included "oversight of City computer operations," the Director did not oversee certain highly sensitive operations, such as the IT vendor's cybersecurity work. The Clerk and Administrator agreed that the Clerk's documented responsibilities needed to be updated.

Documented roles and responsibilities ensure clarity, accountability and efficiency. Inadequate or outdated documentation describing employees' roles and responsibilities increases the risk of unclear roles and noncompliance, which may lead to security risks such as unauthorized access, ineffective incident response and ineffective risk management. In addition, documenting and updating roles and responsibilities enables ongoing institutional knowledge to ensure that City operations would continue with minimal disruption when there is employee turnover.

City employees may inadvertently violate policies when they are not clearly and effectively communicated. Policy violations can result in increased damage by delaying incident response, which could increase remediation costs and the likelihood of data exposure. For example, employees who are not informed of changes to the AUP may be unaware that they are noncompliant with the policy. In addition, when documented cybersecurity roles and responsibilities are unclear, there is an increased risk of cybersecurity gaps, an overreliance on certain individuals and a lack of segregation of incompatible duties, which may lead to ineffective cybersecurity risk management, inefficient incident response and unauthorized access to the City's IT assets and data.

Recommendations

The Council and City officials should:

6. Clearly and effectively communicate policy expectations and updates to all City employees.
7. Periodically review City employee job descriptions and update the descriptions as needed to clearly define designated cybersecurity roles and responsibilities.

Appendix A: Profile, Criteria and Resources

Profile

The City, located in Otsego County, is governed by the elected eight-member Council presided by the Mayor and serves 13,079 residents. The Council is responsible for enacting laws, managing the City's property and controlling the City's finances. The Clerk's responsibilities include serving as the primary IT contact for City employees, monitoring IT vendor services and projects and reviewing user accounts. The Director's responsibilities include City-wide computer oversight. The Administrator is responsible for overseeing each City department, including overall policy compliance.

The City contracts with a third-party vendor for IT services, including user support, network management, and other services provided by one part-time onsite IT specialist and a full-time remote support team that monitors the IT environment and provides support for employees and officials who use City-owned IT assets. City officials rely on the IT vendor to manage the City's IT environment by creating IT and cybersecurity policies and procedures, configuring networks, servers and desktops, providing network devices, creating and managing user accounts, installing software, addressing firewall and antivirus notifications, and responding to any IT-related issues.

City officials and employees use City-owned IT assets (e.g., computers, laptops and tablets) to perform day-to-day operations and access stored information collected by the City. The City 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

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

Officials should provide periodic comprehensive cybersecurity awareness training to help minimize the risk of unauthorized access to IT assets and the misuse or loss of confidential data. Cybersecurity awareness training should explain rules of behavior for using the Internet and the city's IT assets, and communicate related policies and procedures to all IT users. IT asset users need to be aware of cybersecurity risks and be trained in practices that help reduce internal and external threats to IT assets and data. While cybersecurity policies provide guidance for IT users, cybersecurity training helps users understand their roles and responsibilities to ensure IT assets are safeguarded. Training programs should be tailored to a specific audience (e.g., IT asset users or administrators) and include guidance on how to perform their tasks while safeguarding IT assets from cybersecurity threats. Cybersecurity awareness training should reinforce cybersecurity policies and can focus on general security or specific risks, such as the dangers of opening unknown email attachments or downloading files from the Internet.

The Clerk was provided with the 2022 and 2025 information security policies created by the IT vendor, which describes the requirements, including frequency, for conducting risk assessments of the City's information systems. The Clerk provided the 2025 policies to Council Members, the Administrator, and the Director. The Council should ensure officials monitor and document risk assessment results. Monitoring for compliance with the information security policy involves regularly conducting risk assessments, reviewing City IT systems for significant vulnerabilities, tracking new projects, implementing new technologies, and documenting results and decisions made based on those results.

A common council should provide oversight and leadership by adopting cybersecurity policies that consider people, processes and technology; communicating the policies to all IT asset users; and ensuring there are

procedures in place to monitor policy compliance. Cybersecurity policies define a common council's expectations for appropriate IT user behavior, describe the tools and procedures used to help safeguard IT assets from cybersecurity threats, assign key responsibilities and explain the consequences of policy violations. City officials cannot be assured there is adequate protection of the confidentiality, integrity and availability of data and IT assets without ensuring that IT users, or those who manage IT, understand the cybersecurity policies and procedures and their roles and responsibilities related to IT and cybersecurity.

The Council adopted an AUP in 2018 which outlines the technology services, equipment and use of City IT resources and the duties of employees who use City IT resources. The policy states that the City's technology services and equipment are for City business, professional development, communication and publication consistent with the City's mission and goals. Furthermore, officials and employees need to sign an acknowledgment form stating they have read and agree to abide by the AUP. In addition, the IT vendor created the 2022 and 2025 cyber incident response plan that the Clerk, and thereby other City officials, relied on. The plan outlines the steps key personnel should take during a security incident, contact and communication information, response and notification, and proper documentation and follow-up of cyber incidents. City officials should ensure these policies are communicated and distributed to all relevant employees.

Additional Resources

OSC's *Local Government Management Guides*, and other informational resources that are available on OSC's 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 OSC's website to search for audits, resources, publications and training for officials at: <https://www.osc.ny.gov/local-government>.

Appendix B: Response From City Officials

The content below is a reproduced copy of the original response letter issued by City officials, 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.

OFFICE OF THE CITY CLERK

City Hall, 258 Main Street
Oneonta, NY 13820-2589

Phone: 607.432.6450 – **Fax:** 607.433.3420

Internet Address: www.oneonta.ny.us

Email Address: cityinfo@oneonta.ny.us

August 6, 2026

The City of Oneonta appreciates the opportunity to respond to the Office of the State Comptroller's draft cybersecurity audit report. The City takes cybersecurity seriously and welcomes recommendations that improve accountability, continuity, and the protection of public information and systems.

The City accepts that several of its cybersecurity practices could have been more formally documented, centrally maintained and communicated. Corrective steps are already underway. At the same time, the City respectfully disagrees with portions of the draft which characterize shortcomings in documentation and formalization as an absence of the underlying activity. This distinction is important to the accuracy and fairness of the final report.

Audit Scope and Use of 2025 Policy Documents

During fieldwork, the audit team established that its review of City cybersecurity policy requirements would be limited to the City's 2022 policy documentation. The City, along with its IT provider, explained that the 2025 policy had not yet been placed into effect or enforced. The audit team acknowledged that status and advised the City that the 2022 documents would be used because they had directed City practices during the relevant prior period [OSC Comment: See Appendix C, Note 1].

Despite that understanding, in multiple places, the draft report relies on provisions or wording from the 2025 documents to support findings concerning reporting procedures, remediation documentation and other obligations. Most notably, Finding 4 quotes language from the 2025 cyber incident response plan even though the 2022 plan expressly provides for notification of the Oneonta Police Department in the event of a cyber incident. Reliance on the 2025 transition documents creates a different impression of the City's operative reporting expectations [OSC Comment: See Appendix C, Note 1].

As stated in the OSC draft, this audit was conducted in accordance with generally accepted government auditing standards (GAGAS). Within this standard, audit scope is strictly defined and cannot be arbitrarily modified, especially without disclosing the scope change to the subject of the audit. Because the draft report deviates from this expected standard by evaluating the City against out-of-scope materials, the City respectfully rejects all findings and claims that cite alleged non-compliance solely based on the initial version of the 2025 policies [OSC Comment: See Appendix C, Note 1].

Response to Audit Summary

"City officials did not provide adequate governance to safeguard IT assets from cybersecurity threats."

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

The City recognizes OSC's concern regarding formal governance processes, but this opening conclusion is broader than the evidence described in the report. The draft identifies weaknesses principally related to policy adoption, documentation, communication and assignment of responsibilities. It also acknowledges that the City and its IT vendor performed cybersecurity risk assessment activities, established technical controls, sustained a strong vulnerability management program, established a practiced incident response plan, and provided evidence of remediation activity.

The City therefore requests that the summary distinguish between deficiencies in governance documentation and the existence of operational and technical safeguards. A more accurate formulation would state that City officials did not sufficiently formalize, document, and communicate certain elements of cybersecurity governance. That revision would preserve OSC's substantive concerns but without suggesting that the City failed to safeguard its systems generally [OSC Comment: See Appendix C, Note 2].

Finding 1 – Cybersecurity Awareness Training

The City agrees that its prior training process did not consistently ensure or document completion within 30 days of hire and annually thereafter. The City has already implemented a formal cybersecurity awareness training process that includes:

- Cybersecurity awareness training as part of onboarding for new employees;
- Annual cybersecurity awareness training for applicable employees; and
- Central tracking of assignment and completion.

These measures address Recommendation 1 and provide a repeatable process for verifying compliance. The City will continue to review the process and retain completion records.

Finding 2 – Cybersecurity Risk Assessment Documentation

The City agrees that documentation of identified risks, remediation decisions, actions taken, and periodic review could be improved. The final report should, however, preserve the distinction already reflected in the first sentence of Finding 2, "City officials and the City's IT vendor did perform cybersecurity risk assessment activities, including vulnerability management."

During the audit, the City's IT vendor provided materials that included a sample vulnerability report, unprocessed vulnerability data from multiple assessments, and documentation of remediation activities. Those records demonstrate that risks were identified and responsive work occurred. The weakness was that the results, decisions, mitigation steps, and follow-up were not maintained in one centralized, consistently detailed record that allowed City officials to track the entire risk-management lifecycle readily.

Accordingly, the City requests that Finding 2 not be interpreted or summarized as a failure to perform risk assessment activities. The City has worked with its IT vendor to maintain more complete documentation of cybersecurity risk assessment results, including identified risks, recommended mitigation, actions taken, risk-acceptance or deferral decisions where applicable, responsible parties, status, and periodic review by appropriate City officials. This work deals with Recommendation 2 while drawing on the vulnerability-management activities already being performed.

Finding 3 – Adoption, Review and Enforcement of Cybersecurity Policies

The City agrees that its cybersecurity policies should be periodically reviewed, kept current, clearly communicated and supported by documented compliance procedures. The City does not agree, however, that the absence of formal Common Council adoption shows that the policies lacked authority or were not City policies.

The City Charter does not require the Common Council to adopt every internal administrative or operational policy. The City's longstanding practice has been to distinguish between matters requiring legislative action by the Council and policies governing day-to-day administration. Cybersecurity documents provided by the City's IT vendor were treated as operational policies and standards within that administrative structure. The policies

were made available to Council Members for review, and Council Members understood the detailed administration of those policies to remain with City officials and the City's retained IT professionals.

The differing responses OSC received from individual Council Members may demonstrate that there was not a common understanding of whether formal legislative adoption was necessary. Still, they do not establish that the City disregarded its cybersecurity obligations. If OSC maintains Recommendation 3, the City requests that it be framed as a prospective governance recommendation rather than a finding that official Common Council adoption was legally required or that prior operational policies were ineffective solely because the Common Council did not adopt them by resolution [[OSC Comment: See Appendix C, Note 3](#)].

Going forward, the City will continue to conduct periodic policy reviews, correct obsolete titles and authority references, and document monitoring and enforcement activities. These actions address the practical concerns underlying Recommendations 3 through 5 without conceding that the Charter required Council adoption of every internal policy.

The City further notes that information-classification controls were being applied operationally by the City Clerk and the IT vendor. The audit identified that the rationale for classification determinations was not separately and centrally documented and that certain officials were unfamiliar with the policy. Those are valid documentation and communication concerns, but they should not be stated in a manner suggesting that information-classification controls were absent or unenforced.

The Common Council has historically exercised governance over the City's IT operations through its budget, procurement and contracting authority. Following a competitive bidding process, the Common Council votes to award the City's IT services contract and authorizes the engagement of a qualified IT provider to manage the City's day-to-day IT operations, provide technical expertise and implement appropriate safeguards. This structure reflects a decision by the Common Council to retain specialized professional oversight and should not be characterized as an absence of governance merely because individual operational policies were not separately adopted by resolution.

Finding 4 – Policy Communication and Cybersecurity Roles

The City agrees that cybersecurity policies and expectations should be clearly communicated and that assigned responsibilities should be accurately documented. Several IT-related duties evolved as the City's technology environment and vendor relationship developed. Those duties, including acting as a primary IT contact, working with the IT vendor, monitoring IT-related projects and reviewing user accounts, are assigned to City Clerk Harrington through her separate role as IT Liaison. Although she also serves as City Clerk, the IT Liaison duties are not part of, and do not run with, the City Clerk's job description [[OSC Comment: See Appendix C, Note 4](#)].

The Finance Director's job description also assigns oversight of the City's computer operations. In practice, the IT Liaison and Finance Director work in partnership on the City's IT program, with the two roles providing shared oversight and checks and balances rather than responsibility resting with one employee. The City acknowledges that the respective operational and oversight responsibilities of the two roles, including the scope of duties covered by the IT Liaison stipend, have not been described with sufficient specificity.

The City is working to better define and document the scope of duties covered by the IT Liaison stipend to ensure that those responsibilities are accurately defined and described. The City will also periodically review the Finance Director's and other relevant job descriptions, clarify the division of responsibilities, ownership and backup responsibilities, and document the distribution and recognition of cybersecurity policies. These actions address Recommendations 6 and 7 while more accurately documenting the shared oversight structure already in place.

The City specifically objects to the paragraph suggesting that wording in the cyber incident response plan could create inconsistent reporting to law enforcement. That conclusion relies on language from the 2025 transition document. The operative 2022 incident response plan states that the Oneonta Police Department is

to be notified in the event of a cyber incident, which is consistent with the Police Chief's understanding. The quoted 2025 language also addresses variability in external law-enforcement response time and technical capability; it does not direct City employees to withhold incident reports. The City requests that this paragraph be removed or revised to reflect the 2022 plan and the actual reporting expectation [OSC Comment: See Appendix C, Note 1].

Additional Factual Correction

Appendix A states that the City of Oneonta is located in Chautauqua County. The City of Oneonta is located in Otsego County. The City requests correction of this statement in the final report [OSC Comment: See Appendix C, Note 5].

Conclusion

The City appreciates OSC's recommendations and has already begun corrective action. The City's response is not intended to minimize the importance of formal governance, complete documentation, explicit communication, or accountability. Rather, it asks that the final report accurately distinguish among: (1) activities that did not occur; (2) activities that occurred but were not centrally or sufficiently documented; and (3) practices that were operationally implemented but not authorized through the particular approval or job-description mechanism OSC expected.

That distinction will produce a more accurate public record, appropriately recognize the safeguards and risk-management work already performed by City officials and the City's IT vendor, and allow the City's corrective action plan to focus on the actual deficiencies identified.

Finally, the City wishes to recognize the auditors and their supervisor who participated in the on-site fieldwork. Throughout the process, they were professional, responsive and constructive, and the City sincerely appreciated their time, candor and collaborative approach.

Respectfully submitted,

Kerriann Harrington, City Clerk, IT Liaison
City of Oneonta

Appendix C: OSC Comments on the City's Response

Note 1

As noted in the report, GAGAS requires auditors to obtain sufficient, appropriate evidence to provide a reasonable basis for findings and conclusions. City officials provided the City's 2022 and 2025 policies, which were applicable to different portions of our audit scope period. We discussed with City officials the criteria used to assess the City's operations and support our findings and conclusion, including the applicable City policies and the Center for Internet Security (CIS) Critical Security Control 17.

We updated the report to more clearly identify the criteria applicable to each finding. As noted in the report, because the Council did not adopt policies, some City departments were unclear about which policies to follow, which could lead to inconsistent cybersecurity practices among City staff.

Note 2

The report includes seven recommendations that, if implemented, will improve the City's cybersecurity governance, improve accountability for cybersecurity responsibilities, enhance compliance with adopted policies and reduce the risk of unauthorized access, data loss and disruption of critical IT services. In addition, the audit also examined the adequacy of other IT controls. Because of the sensitivity of this information, we communicated it confidentially to City officials.

Note 3

As noted in the report, reviewing policies ensures that they are accurate representations of the Council's expectations, and that the policies clearly define any requirements the Council sets forth to help safeguard IT assets.

Note 4

During the audit period, the Clerk received an annual stipend for certain IT, website and related technology duties. However, her documented responsibilities primarily related to the City's website and did not designate her as the City's IT liaison or assign her responsibility for coordination with the IT vendor regarding the City's overall IT infrastructure.

Note 5

We updated the report to reflect the City's location in Otsego County.

Appendix D: Audit Methodology and Standards

OSC auditors obtained an understanding of internal controls that were deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of the work on internal controls, as well as the work performed in the audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We interviewed Council Members, City officials and employees to gain an understanding of the City's IT operations and related policies, procedures and controls to determine whether the policies and procedures were adopted and effectively implemented, an IT contingency plan existed, and City employees received cybersecurity awareness training. In addition, we interviewed Council Members, City officials and the City's IT vendor about their risk assessment processes to determine whether officials performed risk assessments and properly documented the results.
- We used our professional judgment to select 15 City employees to determine whether they completed cybersecurity awareness training. We used non-biased judgmental sampling to select employees who were present and available to interview on July 18, 2025 to ask them whether they completed the required training.
- We used our professional judgment to select 13 of 168 City computers based on the job titles and duties of the officials and employees who had access to these computers. We selected computers assigned to officials and employees who had access to the City's accounting software, online banking and police evidence, all of which are inherently vulnerable to cybersecurity threats due to the PPSI contained therein. We ran a computerized audit script on the 13 computers on July 18, 2025 and July 25, 2025, and reviewed the Internet history exported by the script to determine whether officials and employees accessed secured and appropriate websites.
- We obtained and reviewed the signed acknowledgement forms on file at the City for a sample of 14 of the 32 employees who were hired within the audit period to determine whether City officials ensured newly hired employees signed the AUP. The sample was selected by choosing the most recent hires during the audit period.
- We analyzed and assessed all 295 enabled network user accounts using a computerized audit script run on July 18, 2025, and compared the network user accounts to the City's employee master listing to determine whether there were any enabled network user accounts assigned to former City employees.

The audit also examined the adequacy of certain IT controls. Because of the sensitivity of some of this information, the results were not discussed in this report but were instead communicated confidentially to City officials.

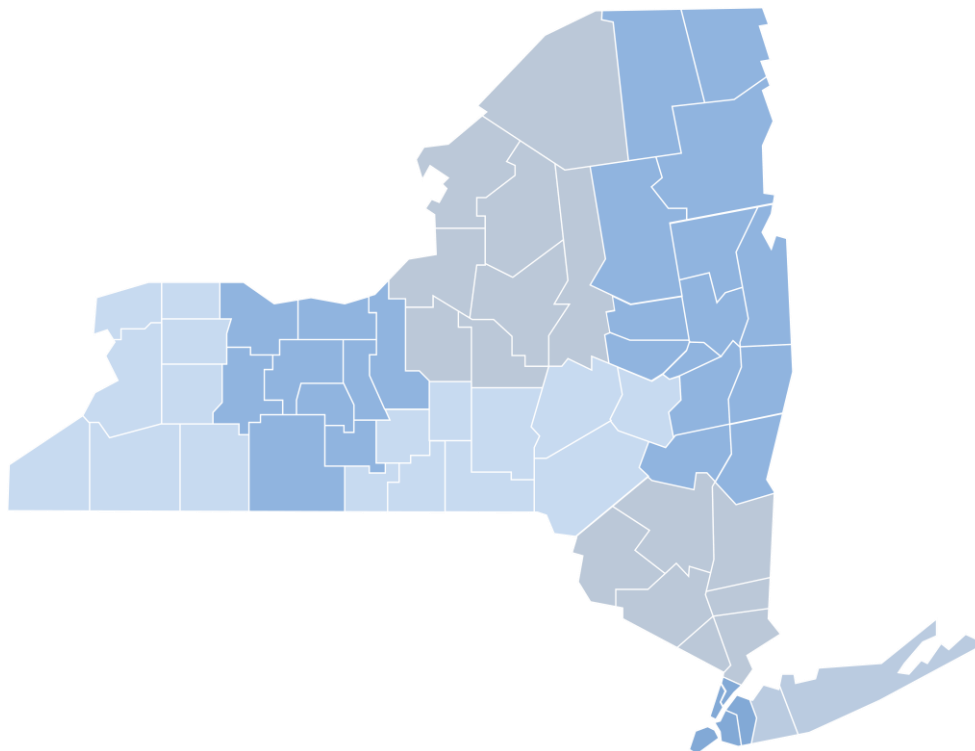
OSC auditors conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. Auditors believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

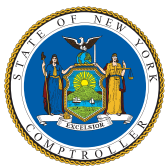
Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or relevant population size and the sample selected for examination.

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

<https://www.osc.ny.gov/>

Prepared by the Division of Local Government and School Accountability



FOLLOW US: [osc.ny.gov/subscribe](https://www.osc.ny.gov/subscribe)