New York State Comptroller
THOMAS P. DiNAPOLI

Wantagh Union Free School District

Financial Application User Access Controls

2024M-46 | October 2024

Division of Local Government and School Accountability

Contents

Report Highlights

Wantagh Union Free School District

Audit Objective

Determine whether the Wantagh Union Free School District (District) Board of Education (Board) and officials established adequate controls over user accounts for the financial application to help prevent inappropriate access and use.

Key Findings

The Board and District officials did not establish adequate controls over user accounts for the financial application to help prevent inappropriate access and use. We determined that the Board and District officials do not have reasonable assurance that they would be able to prevent or detect inappropriate changes to financial data, improper transactions or the misappropriation of funds in the financial application because they did not:

- Develop and adopt policies and procedures related to financial application user accounts and permissions and the review of audit trail reports.
- Limit user account permissions in the financial application to access needed to perform assigned job duties
- Perform an independent review of transactions in the audit trail reports for the system administrator account of the financial application.

Key Recommendations

- Establish adequate policies and procedures related to their financial application.
- Perform an independent review of transactions of the financial application system administrator account on the audit trail reports.
- Assign user account permissions based upon assigned job duties.

District officials generally agreed with our findings and indicated they have initiated or plan to initiate corrective action. Appendix B includes our comments on the District's response.

Audit Period

July 1, 2021 – October 3, 2022

We extended the audit period to January 26, 2023 to review user account activity reports.

Background

The District is located in the Town of Hempstead in Nassau County, and is governed by an elected five-member Board that is responsible for the general management and control of financial and educational affairs. The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The Assistant Superintendent of Business (ASB) is the System Administrator of the District's financial application. The Purchasing Agent is responsible for the authorization to convert requisitions to purchase orders in the financial application. The Director of Information Technology (IT Director) is responsible for overseeing instructional and informational technology for the District.

Quick Facts

Financial Application User Accounts	
Total	117
Active	68
Inactive	49

Financial Application User Access Controls

How Should a Board and District Officials Safeguard Financial Application User Access Controls and Permissions?

A school board (board) and school district (district) officials are responsible for establishing procedures to help secure access to the financial application. To minimize the risk of inappropriate use and access to the financial application, district officials should actively manage application user accounts, including their creation, use and dormancy, and regularly review them to ensure they are still needed.

District officials should have policies and written procedures in place for adding, deleting or modifying individual user account access rights to the financial application. These procedures should establish who has the authority to grant or change access (e.g., department manager approval) and allow users to access only what is necessary to complete their job duties. Policies and procedures help to ensure that computer systems, including financial applications, and the data they process, transmit and store, can be trusted and are available when needed, and that they are adequately protected from inappropriate access and use. Access rights should be updated as necessary, and unneeded (inactive, retired or terminated) user accounts should be disabled in a timely manner.

To help protect a district's computer systems and data, an important control to implement is limiting access to the system administration of the financial application. Users with system administration access can grant user access rights to different modules in the financial application (e.g., payroll, accounts payable, cash receipts) and allows users with this system administration access to set up and modify certain application controls. As a general rule, system administrator access should be granted to a limited number of employees, and employees should only be granted access to modules that they need to perform their job duties. Another important control for monitoring the financial application user account access and use is generating and periodically reviewing audit trail reports. An audit trail records changes made to the system administration of the financial application and records any event where previously recorded data is modified or system parameters are changed, even if temporary. Audit trail reports can be an important detection control for possible manipulation of financial data or other sensitive information.

System administrators should ensure that each financial application user account has a unique username so that access can be appropriately restricted and traced to a specific user. A shared user account, which is an account with a username and password that is shared among two or more people, should be avoided because officials may have difficulty linking any suspicious user account activity to a specific individual. Dormant user accounts are typically defined as accounts which have been inactive for a time period of 45 days or more. Dormant accounts should be disabled because they could indicate a user account that is no longer associated with an active employee and is unnecessary for the performance of duties. System administrators should determine the length of inactivity that indicates a dormant account and terminate accounts that are considered dormant.

The Board and District Officials Did Not Safeguard Financial Application User Access Controls and Permissions

The Board adopted a computer resources and data management policy and accompanying regulations requiring that the Superintendent, in conjunction with the IT Director and ASB, establish procedures governing the management of computer records, including the financial, personnel and student information. These procedures should address passwords, system administration and separation of incompatible duties. However, District officials did not develop written procedures to address these components of data security. As a result, we found weaknesses regarding shared passwords, system administration and separation of duties. The policy did not address procedures for administrating and monitoring the financial application user access, including:

- User account management, including creating, disabling or modifying user accounts.
- User account permissions being limited to only what is required to perform assigned job duties.
- Reviewing audit trail reports for the system administration account.

Because officials did not actively manage or monitor financial application user account access, periodically review user account access or have formal written policies or procedures for granting, changing and disabling user accounts or periodically reviewing user account access to the financial application, District officials did not have reasonable assurance they would be able to detect inappropriate changes to financial data, improper transactions or the misappropriation of funds in the financial application. The ASB told us that there was no process to monitor user account access and he could not explain why there were no processes, written policies or procedures to address these weaknesses, which he inherited when he began working for the District in July 2019. In addition, the ASB stated he was unable to begin to address these issues sooner due to the shift of focus brought on by the COVID-19 pandemic.

We identified seven business office employees (the ASB, Purchasing Agent, Senior Accountant, Payroll Supervisor, Payroll Clerk, Benefits Clerk and a secretary) that were assigned financial application user account permissions that were not required for their assigned job responsibilities.

System Administrator Account Rights – District officials did not properly set up system administrator accounts in the financial application. The ASB and IT Director were both assigned system administrator accounts in the financial application with the ability to modify their own financial application user accounts. Although the IT Director had previously operated as the system administrator of the financial application, she told us that she was not performing this function during the audit period and was not aware that she had an administrative account in the application. We confirmed that the IT Director's administrator account was not used to perform any functions during our review. Therefore, the ASB was the only employee performing the system administrator duties during our audit period and these duties were performed without an independent review of his activities.

As the system administrator, the ASB had the ability to create new user accounts, configure certain system settings and override management controls. He could also change user access, including access to his user account that is separate from his system administrator account, with no oversight to ensure that the modifications were for a valid District purpose. The ASB said he reviews audit trail reports monthly for his system administrator account for changes that he made to user permissions and documents his review by signing and dating a checklist maintained in his office.

Although we reviewed the audit trail reports for the ASB's system administrator account and did not identify any questionable transactions or activity, assigning administrative privileges to an employee who can make financial transactions without an independent review increases the risk of unauthorized changes to accounting records, application security settings and user authorization privileges. These changes could occur and go undetected.

Rights to Add and Delete Employees – Six of the seven financial application user accounts (excluding the secretary) had access to the human resources (HR) and payroll modules with the ability to add and delete employees. Officials from HR were responsible for adding and deleting employee information in the financial application, and these six employees currently do not need this access to perform their assigned job duties. While the secretary did not have the ability to add and delete employees in the financial application, she was able to update employee information in both the HR and payroll modules, within the application. The secretary said she needed this access when she worked in the benefits department, but she transferred to her current position in October 2021 and as of that date no longer needed access to the human resources and payroll modules to perform her current job duties. However, her financial application user account permissions were not updated.

We reviewed audit trail reports for all seven employees and did not identify any instances of adding, deleting or modifying employee information. However, when employees who are not responsible for adding and deleting new employees are granted user account access to do so, there is an increased risk of establishing ghost employees. Furthermore, because some employees can modify pay rates (see next finding “Modifying Pay Rates”), there is an increased risk of paying and then deleting a ghost employee before detection.

Rights to Modifying Pay Rates – The ASB, Purchasing Agent, Senior Accountant and Benefits Clerk had the ability to modify pay rates and salaries in the financial application although it was not required for their job responsibilities. The Benefits Clerk worked in the payroll department until September 2021 when she started working in the benefits department. Her access rights were never modified to align with her current job responsibilities and, as a result, she had more rights than needed to perform her job.

Although we reviewed audit trail reports and determined that these four employees did not modify pay rates or salaries in the financial application, when employees who are not responsible for changing pay rates or salaries are granted user account permissions with the ability to do so, there is an increased risk of unauthorized changes to payroll. The ASB told us that the permissions were predefined based on job titles and not necessarily the employees’ actual responsibilities.

Rights to Convert Requisitions to Purchase Orders – The Senior Accountant was granted the ability to create or increase a purchase order in the financial application, which circumvented the normal purchase order approval process. Purchase orders normally go through a requisition process that entails an employee requesting the needs for goods or services. The request will then go through an approval process, typically through the requestor’s manager. The final step to the process, after it has been approved, requires the Purchasing Agent to review the request and reject or approve the requisition. If approved, it is converted to a purchase order. All increases to existing purchase orders also require the Purchasing Agent’s approval.

Although we reviewed audit trail reports for the Senior Accountant and did not identify any instances of a purchase order being created, we identified 13 instances where the Senior Accountant increased purchase orders by a cumulative total of $197,123, circumventing the Purchasing Agent's approval. For example, she increased a purchase order in May 2022 to procure services from the Board of Cooperative Educational Services by $44,364. Additionally, she increased a purchase order for another vendor by $10,000 in July 2022. The ASB said that while the Senior Accountant was given the same user account access as her predecessor, she should not have been given this access. Although the ASB also said that the Senior Accountant performed these transactions to save time, the Purchasing Agent's approval process should not be circumvented for convenience.

Rights to Override Non-Payroll Payments – Although the Purchasing Agent's job responsibilities did not include processing payments, she was granted rights to override system controls. The Purchasing Agency could process payments even when the approved purchase order or budgeted appropriation may not have sufficient funds. However, if there were insufficient appropriations in the budget code, a budget transfer would have to be approved and then performed to increase the budget code and allow the purchase order to be approved.

We reviewed the audit trail reports and identified five payments totaling $698,534 where the Purchasing Agent overrode the financial application to process payments. This resulted in budget codes being over expended by $58,559 and purchase orders being over expended by $46,359. The Purchasing Agent said this was done to save time so the payment could be processed without making a budget transfer or increasing the purchase order. For example, one payment totaling $37,114 from the special aid fund only had available appropriations of $24,486, resulting in the budget code being over expended by $12,628. The ASB said that budget codes in the special aid fund are often over expended because the money comes from State or federal aid, and he is not as concerned that budget estimates are as accurate as in other funds. The ASB also said that these budget codes and appropriations were overspent to save time, which allowed the payments to be processed without performing the necessary budget transfer or increasing the purchase order. He acknowledged that the Purchasing Agent should not have been granted the ability to process cash disbursements.

The ASB acknowledged that the excessive user permissions in the financial application for the seven employees reviewed (including himself) were not required for their job responsibilities and that he is in the process of updating the permissions, as a result of our audit inquiry. The original permissions were predefined based on job titles and not necessarily the employees' actual responsibilities.

Active Dormant and Shared User Accounts – The District had four dormant user accounts (one of which was a shared user account) in the financial application that were not disabled, removed or monitored. We reviewed 68 active financial application user accounts to determine whether the accounts and their permissions were needed and adequately monitored, and identified four dormant and shared accounts that should have been disabled, including:

- A temporary purchasing user account that was used by multiple employees when the purchasing clerk was out on leave. Instead of assigning a user account and permissions to each employee as needed, this account and password was shared by clerical staff to perform purchasing functions, such as manually converting requisitions to purchase orders after it was authorized by the Purchasing Agent and printing approved purchase orders to be mailed out to vendors. This shared user account was active but last used in December 2021 and, therefore, not needed. The ASB could not identify which clerical employee used the account to perform the various functions that were performed when the purchasing clerk was out on leave. He said that because there were different staff members assisting with performing tasks, it was easier to assign a generic (shared) user account than to change access each day for different users.

- A test account was created for the ASB to review different financial application settings, including confirming permission settings prior to granting permissions. This account was used periodically during the audit period but was not deactivated when not being used. For example, this account was not used for almost six consecutive months, from November 2, 2021 to April 28, 2022.
- A user account was assigned to the District's internal auditors (non-employees) with read-only abilities to view various transactions and reports. During the audit period, this account was only used on July 13, 2022 and was not deactivated when not being used.
- A user account was assigned to the District's external auditors (non-employees) to review various transactions and reports. This account was used twice during our audit period (July 2021 and May 2022), and was not deactivated when not being used.

Because District officials did not require each user to have a unique username and password and disable dormant or temporary accounts, there was an increased risk that sensitive information could be accessed and unauthorized or inappropriate activity could occur within the financial application. Additionally, when users share an account, accountability is diminished and questionable activity within the financial application may be difficult to trace to a specific user.

What Do We Recommend?

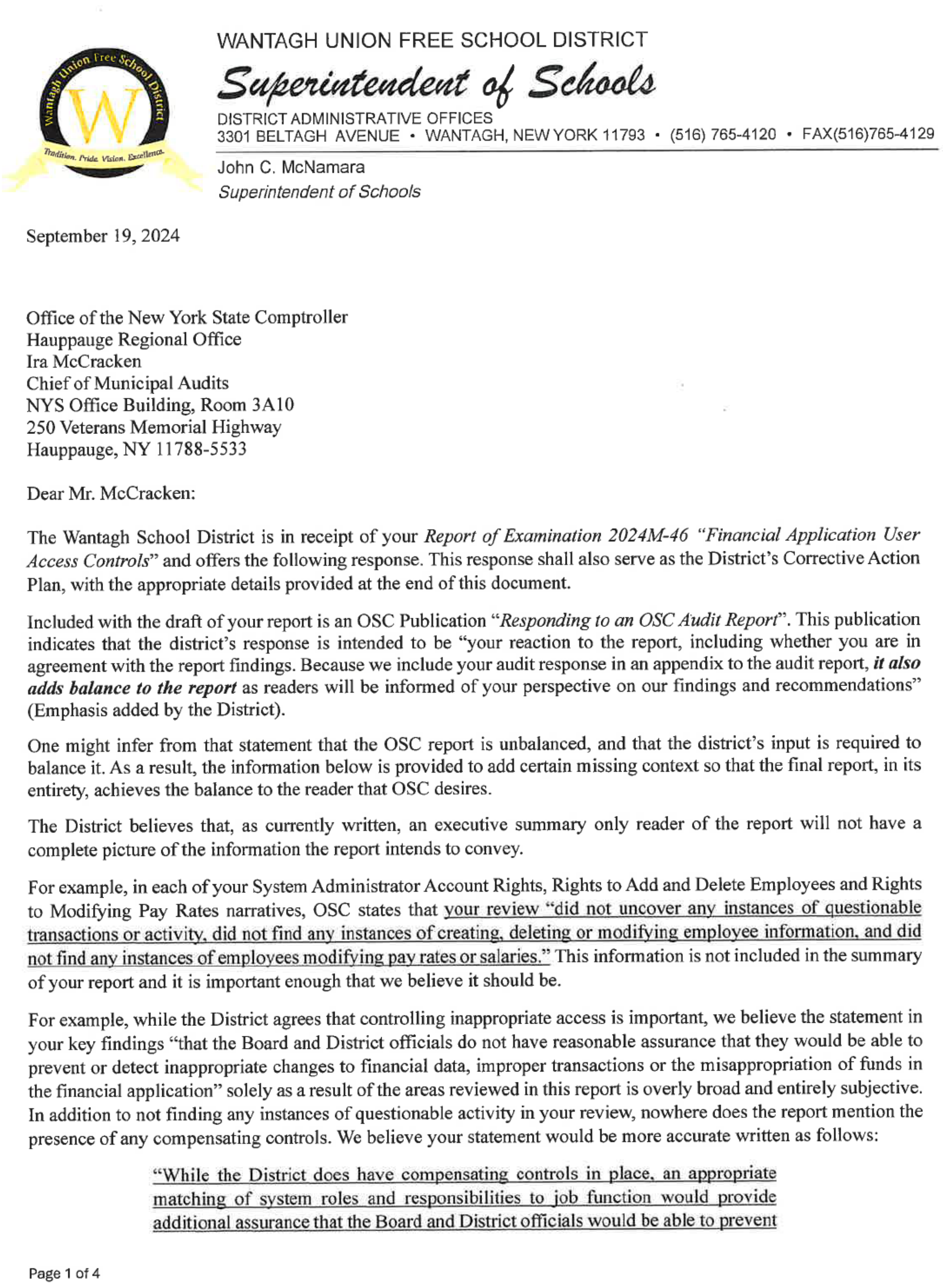
The Board should:

1. Develop and adopt policies and written procedures to address financial application access, including guidance for user accounts, user permissions and reviewing audit trail reports.
2. Ensure that an independent review of the audit trail reports for system administrator user accounts in the financial application is performed.
3. Ensure that system administrator user account permissions in the financial application are only granted to employees who are assigned to perform the job responsibilities.

District officials and the IT Director should:

4. Review financial application user permissions, including the ability to override application controls, and ensure that the permissions are granted based upon job duties.
5. Periodically review user permission reports in the financial application and deactivate user accounts that are dormant or not being used.
6. Avoid the use of shared accounts in the financial application, and ensure each user has a unique username and password.

Appendix A: Response From District Officials



WANTAGH UNION FREE SCHOOL DISTRICT
Superintendent of Schools
DISTRICT ADMINISTRATIVE OFFICES
3301 BELTAGH AVENUE • WANTAGH, NEW YORK 11793 • (516) 765-4120 • FAX(516)765-4129

John C. McNamara
Superintendent of Schools

September 19, 2024

Office of the New York State Comptroller
Hauppauge Regional Office
Ira McCracken
Chief of Municipal Audits
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, NY 11788-5533

Dear Mr. McCracken:

The Wantagh School District is in receipt of your *Report of Examination 2024M-46 "Financial Application User Access Controls*" and offers the following response. This response shall also serve as the District's Corrective Action Plan, with the appropriate details provided at the end of this document.

Included with the draft of your report is an OSC Publication "*Responding to an OSC Audit Report*". This publication indicates that the district's response is intended to be "your reaction to the report, including whether you are in agreement with the report findings. Because we include your audit response in an appendix to the audit report, ***it also adds balance to the report*** as readers will be informed of your perspective on our findings and recommendations" (Emphasis added by the District).

One might infer from that statement that the OSC report is unbalanced, and that the district's input is required to balance it. As a result, the information below is provided to add certain missing context so that the final report, in its entirety, achieves the balance to the reader that OSC desires.

See Note 1 Page 11

The District believes that, as currently written, an executive summary only reader of the report will not have a complete picture of the information the report intends to convey.

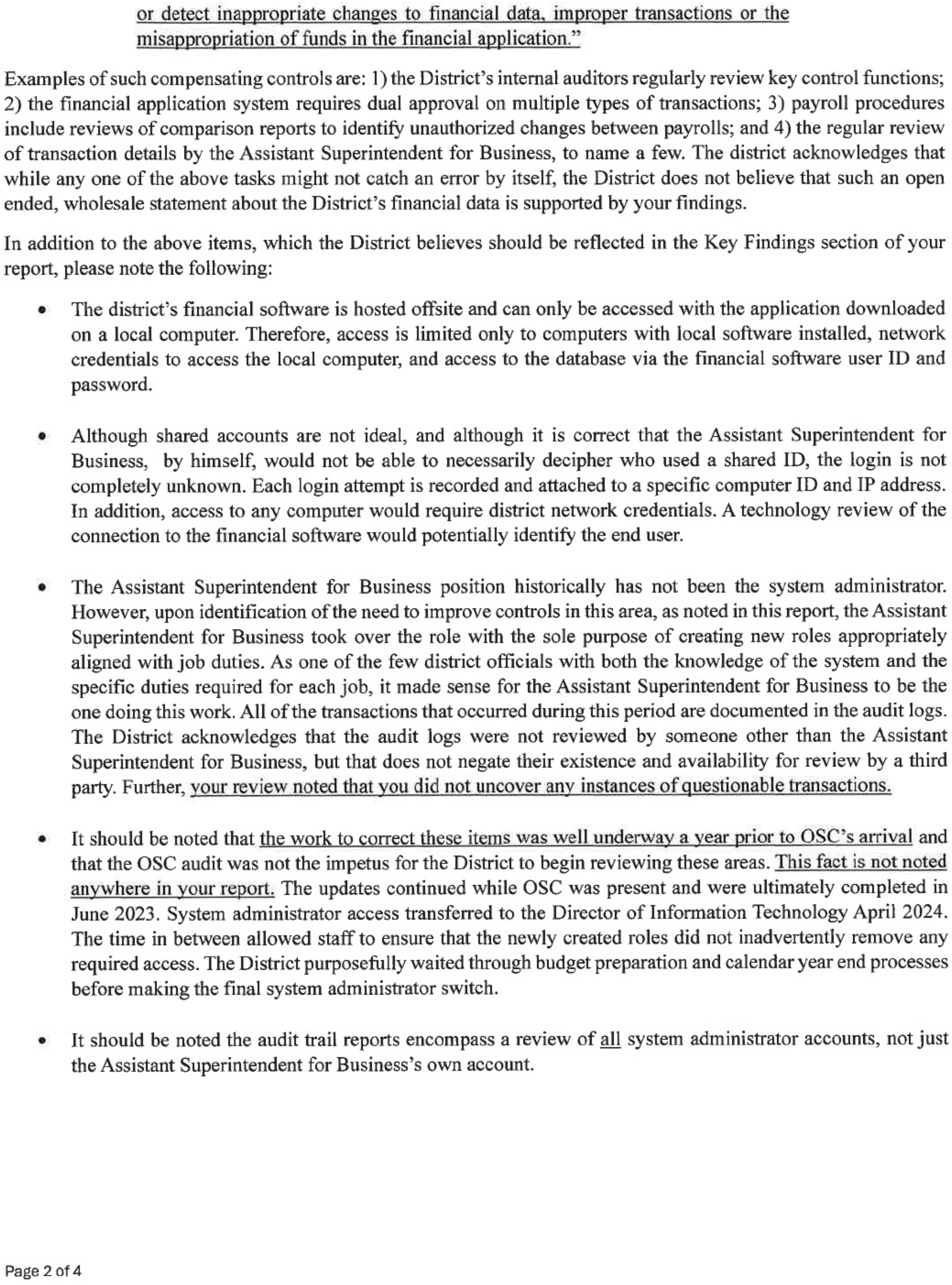
For example, in each of your System Administrator Account Rights, Rights to Add and Delete Employees and Rights to Modifying Pay Rates narratives, OSC states that your review "did not uncover any instances of questionable transactions or activity, did not find any instances of creating, deleting or modifying employee information, and did not find any instances of employees modifying pay rates or salaries." This information is not included in the summary of your report and it is important enough that we believe it should be.

For example, while the District agrees that controlling inappropriate access is important, we believe the statement in your key findings "that the Board and District officials do not have reasonable assurance that they would be able to prevent or detect inappropriate changes to financial data, improper transactions or the misappropriation of funds in the financial application" solely as a result of the areas reviewed in this report is overly broad and entirely subjective. In addition to not finding any instances of questionable activity in your review, nowhere does the report mention the presence of any compensating controls. We believe your statement would be more accurate written as follows:

See Note 2 Page 11

> "While the District does have compensating controls in place, an appropriate matching of system roles and responsibilities to job function would provide additional assurance that the Board and District officials would be able to prevent

Page 1 of 4



or detect inappropriate changes to financial data, improper transactions or the misappropriation of funds in the financial application."

Examples of such compensating controls are: 1) the District's internal auditors regularly review key control functions; 2) the financial application system requires dual approval on multiple types of transactions; 3) payroll procedures include reviews of comparison reports to identify unauthorized changes between payrolls; and 4) the regular review of transaction details by the Assistant Superintendent for Business, to name a few. The district acknowledges that while any one of the above tasks might not catch an error by itself, the District does not believe that such an open ended, wholesale statement about the District's financial data is supported by your findings.

In addition to the above items, which the District believes should be reflected in the Key Findings section of your report, please note the following:

- The district's financial software is hosted offsite and can only be accessed with the application downloaded on a local computer. Therefore, access is limited only to computers with local software installed, network credentials to access the local computer, and access to the database via the financial software user ID and password.

- Although shared accounts are not ideal, and although it is correct that the Assistant Superintendent for Business, by himself, would not be able to necessarily decipher who used a shared ID, the login is not completely unknown. Each login attempt is recorded and attached to a specific computer ID and IP address. In addition, access to any computer would require district network credentials. A technology review of the connection to the financial software would potentially identify the end user.

See Note 3 Page 11

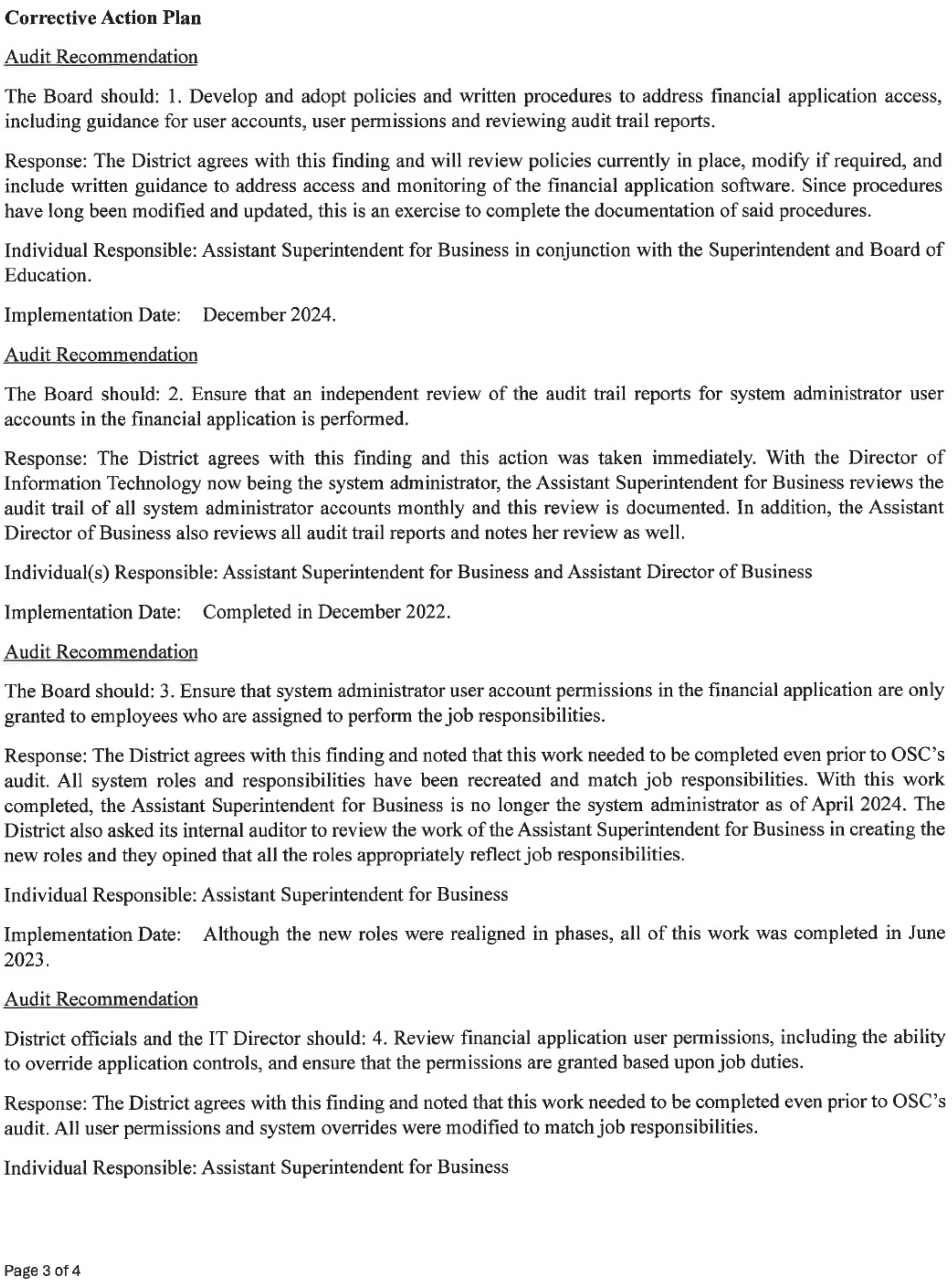
- The Assistant Superintendent for Business position historically has not been the system administrator. However, upon identification of the need to improve controls in this area, as noted in this report, the Assistant Superintendent for Business took over the role with the sole purpose of creating new roles appropriately aligned with job duties. As one of the few district officials with both the knowledge of the system and the specific duties required for each job, it made sense for the Assistant Superintendent for Business to be the one doing this work. All of the transactions that occurred during this period are documented in the audit logs. The District acknowledges that the audit logs were not reviewed by someone other than the Assistant Superintendent for Business, but that does not negate their existence and availability for review by a third party. Further, your review noted that you did not uncover any instances of questionable transactions.

See Note 2 Page 11

- It should be noted that the work to correct these items was well underway a year prior to OSC's arrival and that the OSC audit was not the impetus for the District to begin reviewing these areas. This fact is not noted anywhere in your report. The updates continued while OSC was present and were ultimately completed in June 2023. System administrator access transferred to the Director of Information Technology April 2024. The time in between allowed staff to ensure that the newly created roles did not inadvertently remove any required access. The District purposefully waited through budget preparation and calendar year end processes before making the final system administrator switch.

See Note 4 Page 11

- It should be noted the audit trail reports encompass a review of all system administrator accounts, not just the Assistant Superintendent for Business's own account.



Corrective Action Plan

Audit Recommendation

The Board should: 1. Develop and adopt policies and written procedures to address financial application access, including guidance for user accounts, user permissions and reviewing audit trail reports.

Response: The District agrees with this finding and will review policies currently in place, modify if required, and include written guidance to address access and monitoring of the financial application software. Since procedures have long been modified and updated, this is an exercise to complete the documentation of said procedures.

Individual Responsible: Assistant Superintendent for Business in conjunction with the Superintendent and Board of Education.

Implementation Date: December 2024.

Audit Recommendation

The Board should: 2. Ensure that an independent review of the audit trail reports for system administrator user accounts in the financial application is performed.

Response: The District agrees with this finding and this action was taken immediately. With the Director of Information Technology now being the system administrator, the Assistant Superintendent for Business reviews the audit trail of all system administrator accounts monthly and this review is documented. In addition, the Assistant Director of Business also reviews all audit trail reports and notes her review as well.

Individual(s) Responsible: Assistant Superintendent for Business and Assistant Director of Business

Implementation Date: Completed in December 2022.

See Note 5 Page 11

Audit Recommendation

The Board should: 3. Ensure that system administrator user account permissions in the financial application are only granted to employees who are assigned to perform the job responsibilities.

Response: The District agrees with this finding and noted that this work needed to be completed even prior to OSC's audit. All system roles and responsibilities have been recreated and match job responsibilities. With this work completed, the Assistant Superintendent for Business is no longer the system administrator as of April 2024. The District also asked its internal auditor to review the work of the Assistant Superintendent for Business in creating the new roles and they opined that all the roles appropriately reflect job responsibilities.

Individual Responsible: Assistant Superintendent for Business

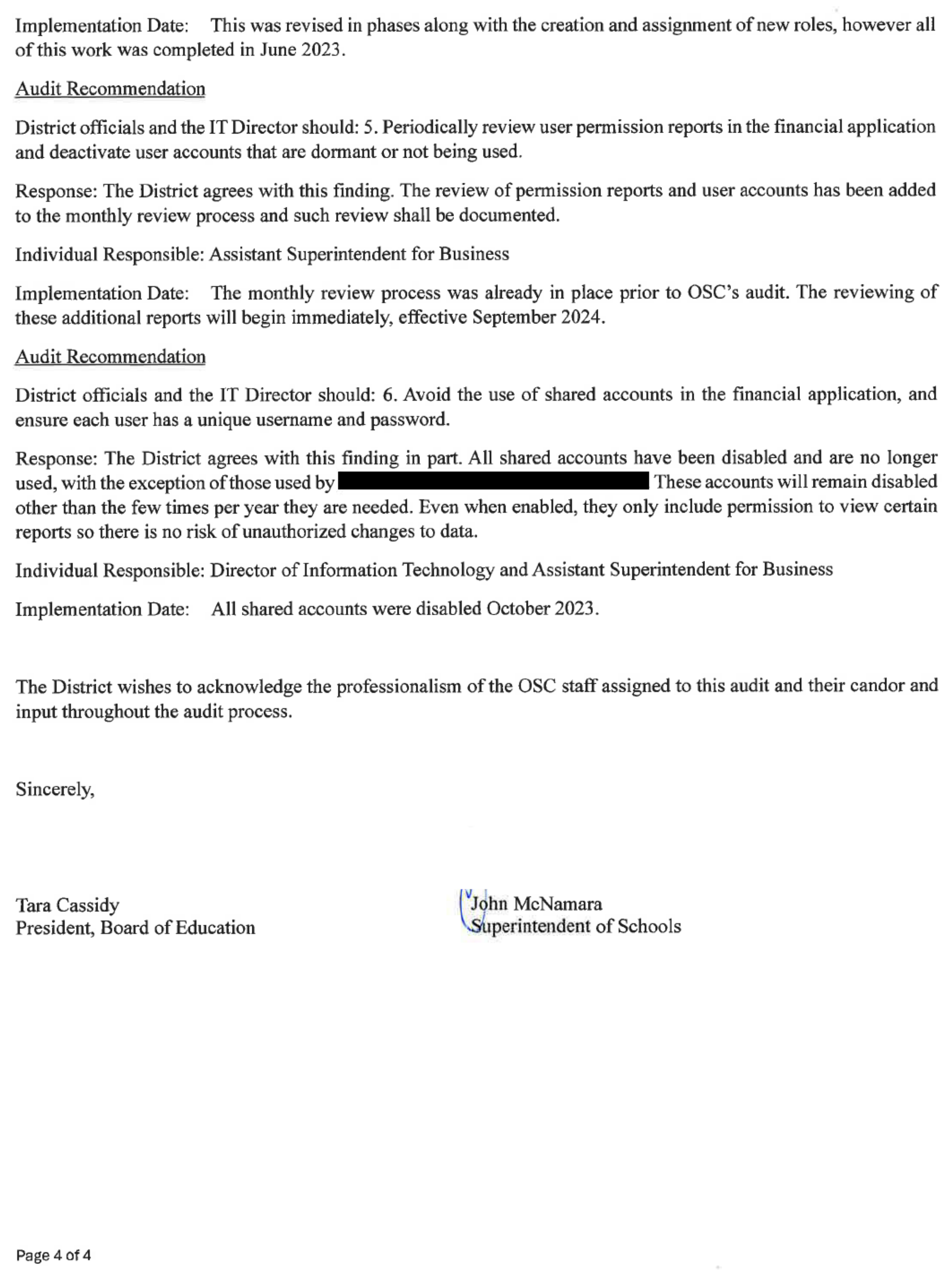
Implementation Date: Although the new roles were realigned in phases, all of this work was completed in June 2023.

Audit Recommendation

District officials and the IT Director should: 4. Review financial application user permissions, including the ability to override application controls, and ensure that the permissions are granted based upon job duties.

Response: The District agrees with this finding and noted that this work needed to be completed even prior to OSC's audit. All user permissions and system overrides were modified to match job responsibilities.

Individual Responsible: Assistant Superintendent for Business



Implementation Date: This was revised in phases along with the creation and assignment of new roles, however all of this work was completed in June 2023.

Audit Recommendation

District officials and the IT Director should: 5. Periodically review user permission reports in the financial application and deactivate user accounts that are dormant or not being used.

Response: The District agrees with this finding. The review of permission reports and user accounts has been added to the monthly review process and such review shall be documented.

Individual Responsible: Assistant Superintendent for Business

Implementation Date: The monthly review process was already in place prior to OSC's audit. The reviewing of these additional reports will begin immediately, effective September 2024.

Audit Recommendation

District officials and the IT Director should: 6. Avoid the use of shared accounts in the financial application, and ensure each user has a unique username and password.

Response: The District agrees with this finding in part. All shared accounts have been disabled and are no longer used, with the exception of those used by [redacted] These accounts will remain disabled other than the few times per year they are needed. Even when enabled, they only include permission to view certain reports so there is no risk of unauthorized changes to data.

Individual Responsible: Director of Information Technology and Assistant Superintendent for Business

Implementation Date: All shared accounts were disabled October 2023.

The District wishes to acknowledge the professionalism of the OSC staff assigned to this audit and their candor and input throughout the audit process.

Sincerely,

Tara Cassidy
President, Board of Education

John McNamara
Superintendent of Schools

Appendix B: OSC Comments on the District's Response

Note 1

Our publication's statement was not written to infer that our report is unbalanced. It is important to have the District's perspective so the reader can understand the District's position related to the audit findings and recommendations.

Note 2

Our report did identify instances of questionable activities, such as the Purchasing Agent overriding system controls to process payments which in some instances resulted in budget codes being over expended. Although the compensating controls discussed in the District's response are relevant, they generally represent controls which can identify unusual transactions that have occurred. Our audit objective was to help prevent inappropriate access and use in the financial application from occurring.

Note 3

As indicated in the report, each financial application user should have a unique username so that access can be restricted and traced to a specific user, not to a computer.

Note 4

The excessive user permissions mentioned in our audit report were identified on the user permissions report printed on October 3, 2022, which was after field work began. District officials did not provide us with updated reports showing that the user access of these individuals was modified. Therefore, we did not find any evidence that District officials were working to correct the items listed in our report prior to the beginning of our fieldwork.

Note 5

The December 2022 implementation date in the District's response is not accurate. The January 2023 audit trail reports were initialed as reviewed by the ASB. In March 2023, the ASB told us that the Assistant Director of Business (Purchasing Agent) was reviewing and signing off on the reports but did not provide support to substantiate this assertion.

Appendix C: Audit Methodology and Standards

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

- We reviewed the District's computer resources and data management policy and accompanying regulations to determine whether they were adequate, and interviewed District employees to gain an understanding of the procedures related to the financial application user account management and monitoring.
- We interviewed an employee of the financial application's company to gain an understanding of what various user account permissions gave the employee the ability to do.
- We interviewed District officials and employees from the business office to gain an understanding of employee job duties/functions. We reviewed financial application user permissions to determine whether user account access was assigned based upon job duties. We also reviewed audit trail reports to determine whether any employees had excessive access.
- We reviewed a list of 117 financial application user accounts to determine whether there were generic (shared) accounts and accounts assigned to District employees or non-employees. We also reviewed the financial application logon activity reports for the four dormant user accounts to determine whether the accounts were being used or could have been disabled.

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 size of the relevant population and the sample selected for examination.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. 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. The CAP should be posted on the District's website for public review.

Appendix D: Resources and Services

Regional Office Directory
www.osc.ny.gov/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.ny.gov/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.ny.gov/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.ny.gov/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.ny.gov/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.ny.gov/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.ny.gov/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.ny.gov/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.ny.gov/local-government/academy

Contact

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

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief of Municipal Audits

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533

Tel (631) 952-6534 • Fax (631) 952-6091 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties