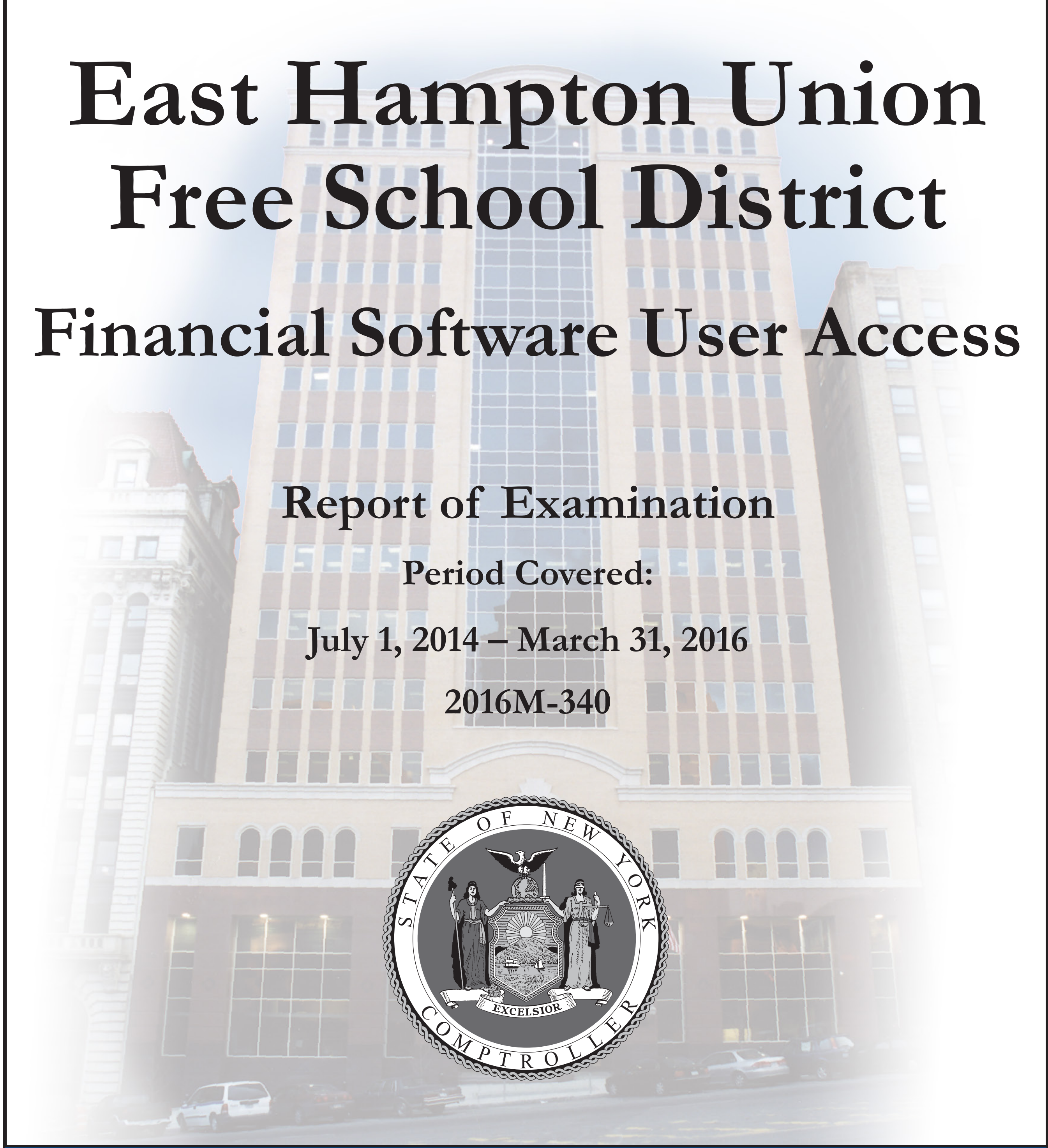
Office of the New York State Comptroller

Division of Local Government
& School Accountability



East Hampton Union Free School District

Financial Software User Access

Report of Examination

Period Covered:

July 1, 2014 – March 31, 2016

2016M-340

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

December 2016

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help school district officials manage their districts efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as district's compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving district operations and Board of Education governance. Audits also can identify strategies to reduce district costs and to strengthen controls intended to safeguard district assets.

Following is a report of our audit of the East Hampton Union Free School District, entitled Financial Software User Access. This audit was conducted 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.

This audit's results and recommendations are resources for district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

Introduction

Background

The East Hampton Union Free School District (District) is located in the Town of East Hampton in Suffolk County. The District is governed by the Board of Education (Board), which is composed of seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools 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 District operates three schools and has approximately 1,800 students and 485 employees. For the 2014-15 fiscal year, the District spent approximately $63.6 million. The District's budgeted appropriations for the 2015-16 fiscal year were approximately $66.1 million, funded primarily with State aid, real property taxes, tuition from other districts and grants.

The District uses a vendor software package for the majority of its financial operations, including cash receipts, cash disbursements, budget transfers and employee payroll. The Network System Manager is responsible for maintaining the District's financial software.

Objective

The objective of our audit was to evaluate the District's controls over user access to the financial software. Our audit addressed the following related question:

- Have District officials taken appropriate action to safeguard District information when establishing and monitoring user accounts within the District's financial software?

Scope and Methodology

We examined the District's control over user access to the financial software for the period July 1, 2014 through March 31, 2016. Our audit also examined the adequacy of certain information technology (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 District officials.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix B of this report. 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.

Comments of District Officials and Corrective Action

The results of our audit and recommendations have been discussed with District officials, and their comments, which appear in Appendix A, have been considered in preparing this report. District officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

The Board has the responsibility to initiate corrective action. 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, 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, with a copy forwarded to 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 Board should make the CAP available for public review in the District Clerk's office.

Financial Software User Access

District officials are responsible for designing internal controls over IT that include policies and procedures to protect software and data from unauthorized access and loss or misuse due to errors, malicious intent or accidents. Such policies and procedures should specify that users of the financial software system have access to only the applications needed to perform their job duties. Additionally, the periodic review of audit logs is an important control for detecting possible manipulation of financial data or other sensitive information. Both the review of audit logs and system administration should be assigned to individuals who are independent of financial transactions.

The Board adopted a computer control policy[1] that establishes procedures for granting access rights to the financial software. The policy requires that a system administrator be designated by the Board each year. The system administrator should report to the Assistant Superintendent for Business and has authority to change user account permissions and account code access for all user accounts in the financial software. The system administrator, with written approval of the Assistant Superintendent for Business, is responsible for creating, maintaining and managing permissions and removing user accounts as directed by the Assistant Superintendent for Business. The system administrator should maintain backup documentation of all user account creations and modifications and provide the Assistant Superintendent for Business with user change reports monthly. User permissions are required to be granted based on job duties and proper segregation of duties. The Assistant Superintendent for Business and system administrator are required to review permissions quarterly to ensure a proper segregation of duties and report to the Board. Finally, audit trails for system maintenance are required to be provided to the Board quarterly.

District officials did not comply with the Board's computer control policy. The Board has not annually designated a system administrator. Instead, the Board annually appoints a Network Systems Manager who performs these duties. As a result, there may be confusion as to who is responsible for financial software administration. Also, District officials have not adopted procedures outlining how user access rights should be established or modified, and permissions are not reviewed quarterly to ensure a proper segregation of duties. Further, change reports are not provided to the Assistant Superintendent for Business monthly and audit trails are not reviewed or provided to the Board.

[1] The policy was adopted on May 21, 2013.

We looked at all fifty users of the District's financial software and found that three users, including the Assistant Superintendent for Business, were granted system administrator access even though it was not required to perform their job duties. Also, District officials provided leave record, vendor record, budget transfer and personal, private and sensitive information (PPSI) access rights to 18[2] users that did not require it to perform their job duties. Finally, District officials do not review audit logs and change reports or provide audit trails to the Board on a quarterly basis.

System Administrators — An individual who has financial system administrative rights can add new users, configure certain system settings, override management controls, create and change user access rights and record and adjust entries. Accordingly, the financial system administrator should not be involved in financial operations. If this is not feasible, then system activity should be periodically reviewed, and audit logs should be generated and reviewed on a regular basis.

The Network Systems Manager and four other users were granted financial system administrator rights, including the Eastern Suffolk Board of Cooperative Education of Services (ESBOCES), the Assistant Superintendent for Business, the software vendor and the Director of Learning Technology and Instruction.

The Network Systems Manager required this access to manage the system, and District officials told us that ESBOCES required this access to back up the financial data on a daily basis. However, the Assistant Superintendent for Business, the software vendor and the Director of Learning Technology and Instruction did not need system administration access.

District officials told us that the Assistant Superintendent for Business was granted system administration rights when the District was notified of our audit. The Assistant Superintendent for Business needed the access to send the data requested by our Office but was not removed as system administrator after the data had been sent. With administrative rights, the Assistant Superintendent for Business has the ability to add, delete and modify records in all functions of the financial software. In addition, she can grant user access, override controls and make changes to the system that may enable her to make intentional or unintentional changes. When we brought this to the attention of District officials, they removed the Assistant Superintendent for Business as a system administrator.

[2] Some users had access to more than one software module.

District officials told us that the software vendor required administration rights when the financial software was upgraded in August 2014 to add users, help with implementation and perform system updates and maintenance. District officials also told us that the Director of Learning Technology and Instruction was the backup to the Network Systems Manager and helped with resolving problems when the upgrade was implemented. Because some users may require access for only a limited time, District officials should review administration access and determine who needs administrative rights on a regular basis.

We also determined that no one maintains back-up documentation of user account creations and modifications or routinely generates and reviews financial software audit logs and change reports to monitor user activity and compliance with computer use policies. Additionally no one provides the Assistant Superintendent for Business with monthly user change reports or the Board with audit trails for system maintenance on a quarterly basis.

We reviewed the audit trail for system administration transactions and found the ESBOCES and the Assistant Superintendent for Business did not add, delete or modify any users and that the Network Systems Manager, software vendor and the Director of Learning Technology did not inappropriately assign rights or users. Although we did not find any inappropriate system administration transactions, this type of access could allow users to make unauthorized changes to the accounting records, financial software security settings and user access rights. Therefore, the District should limit the number of system administrators to those who need it to perform their job duties.

<u>Leave Records</u> — Fourteen users, including the software vendor, can add, delete or modify leave records in the financial software. Each of the District's three school buildings and the Business Office have a designated individual who maintains the leave records for the building. There are backup employees for each of the individuals in the event that they are on vacation or otherwise unavailable. However, there are an additional five individuals who have access to add, delete or modify leave records. Because they are not responsible for entering leave records, these individuals do not need this access to perform their job duties. Employees who require this access to perform their job duties should not be allowed to enter, modify or delete information for their own leave time records.

We reviewed the leave records and accruals for 15[3] employees to determine if leave used was properly deducted from their leave

[3] Thirteen employees with access to the module (including the Assistant Superintendent for Business) and two employees with system administrator rights (Network Systems Manager and the Director of Learning Technology and Instruction)

accruals. We found minor errors with four of the employees' leave accruals. For example, two employees deleted a vacation day used from their own leave time records. Although we later determined that these leave days were used on a District holiday, these individuals should not have been able to delete information from their own leave time records. By allowing access to District leave records, there is an increased risk of unauthorized modifications, deletions or additions to time records, and individuals could use or be paid for leave time for which they are not entitled.

Vendor Records — Seven District employees can add, delete or modify purchase orders and vendor information. However, only two users, the Secretary to the Assistant Superintendent for Business and the Assistant Superintendent for Business, need access to purchase orders and vendor information to perform their job duties. We reviewed 135 claims totaling $584,262 to confirm that the ordering and shipping addresses were the District's address, that vendor names and addresses were consistent throughout and that purchases were for valid expenditures. Although we found no discrepancies, this type of access could allow users to create fictitious vendors and issue purchase orders to those vendors for personal goods and services.

We also reviewed audit trails for nine[4] District employees. Seven users made no changes to vendor information, one user changed a phone number and another user added 20 vendors during the audit period. Although the change to one vendor and addition of 20 vendors was appropriate, by allowing excess user access to vendor records, District officials increase the risk that fictitious vendors could be added or vendor records could be inappropriately changed, resulting in inappropriate payments. District officials told us the individual who added vendors required access because she was a backup to the employee who was responsible for adding vendors. After we brought this to the attention of District officials, they removed her permissions because she no longer required access to add vendors.

Budget Transfers — Nine users, including the software vendor, can add, delete or modify budget transfers. However, only two users, the Senior Clerk and the Assistant Superintendent for Business, needed access to budget transfers in the financial software to perform their job duties. Allowing users who do not need access to budget transfers increases the risk that budget transfers could be made without proper authorization and approval. We reviewed transfers for December 2014

[4] Seven employees with vendor access (including the Assistant Superintendent for Business) and two employees with system administrator rights (Network Systems Manager and the Director of Learning Technology and Instruction)

and September 2015[5] and found the Senior Clerk made 16 transfers totaling $1,747,966. All 16 transfers were properly authorized and approved by the Assistant Superintendent for Business.

We also reviewed audit trails for the seven users who did not need access to budget transfer transactions to perform their job duties. One user (the Treasurer) made three budget transfers on August 22, 2015. The Assistant Superintendent for Business stated that these transfers were done as part of year-end procedures and that the Treasurer is her backup to do year-end journal entries. Therefore, according to District officials, three of the nine individuals need access to budget transfers on a regular basis. However, because the Treasurer does not require this access year round, it should be removed and restored for only as long as she needs it to do year-end journal entries. Allowing excess users the ability to make budget transfers increases the risk of unauthorized budget transfers resulting in expenditures exceeding what the Board intended.

Personal, Private and Sensitive Information — PPSI is any information to which unauthorized access, disclosure, modification, destruction or disruption of access or use could severely impact critical functions, employees, customers, third parties, or citizens of New York in general. Private information could include one or more of the following: social security number; driver's license number or non-driver ID; account number; credit card number; debit card number and security code; or access code/password that permits access to an individual's financial account or protected student records. The ability to access PPSI should be limited to those employees who need access to perform their job duties.

Seven users had access to view employees' entire social security numbers. District officials explained that it was necessary for two users to have access to view the entire social security numbers to perform their job duties. Therefore, five users did not require this access. Allowing access to sensitive District data increases the risk that PPSI may be lost or compromised.

The District transitioned to new financial software during the summer of 2014. The first day the new system was used was September 3, 2014. District officials told us that they had encountered problems with restricting user permissions when transitioning to the new financial software. They told us that when they attempted to restrict access to permissions that were not related to users' job duties, the users were unable to access permissions to areas they needed access to for their job duties.

[5] See Appendix B for methodology.

Due to the improper assignment of system administrative rights and access rights for leave records, vendor information, budget transfers and PPSI and the lack of review of logs, change reports and audit trails, there is an increased risk that unauthorized changes to the accounting records, software security settings and user authorization privileges could occur and go undetected. This could lead to the loss or exposure of important financial data and cause interruptions to District operations.

Recommendations

The Board should:

1. Annually designate an administrator for the financial software to clarify who is responsible for financial software administration.

District officials should:

2. Develop written procedures outlining how user access rights should be established or modified based on job duties and proper segregation of duties.

3. Review permissions to ensure a proper segregation of duties and report to the Board on a quarterly basis.

4. Limit the number of users with system administrator rights.

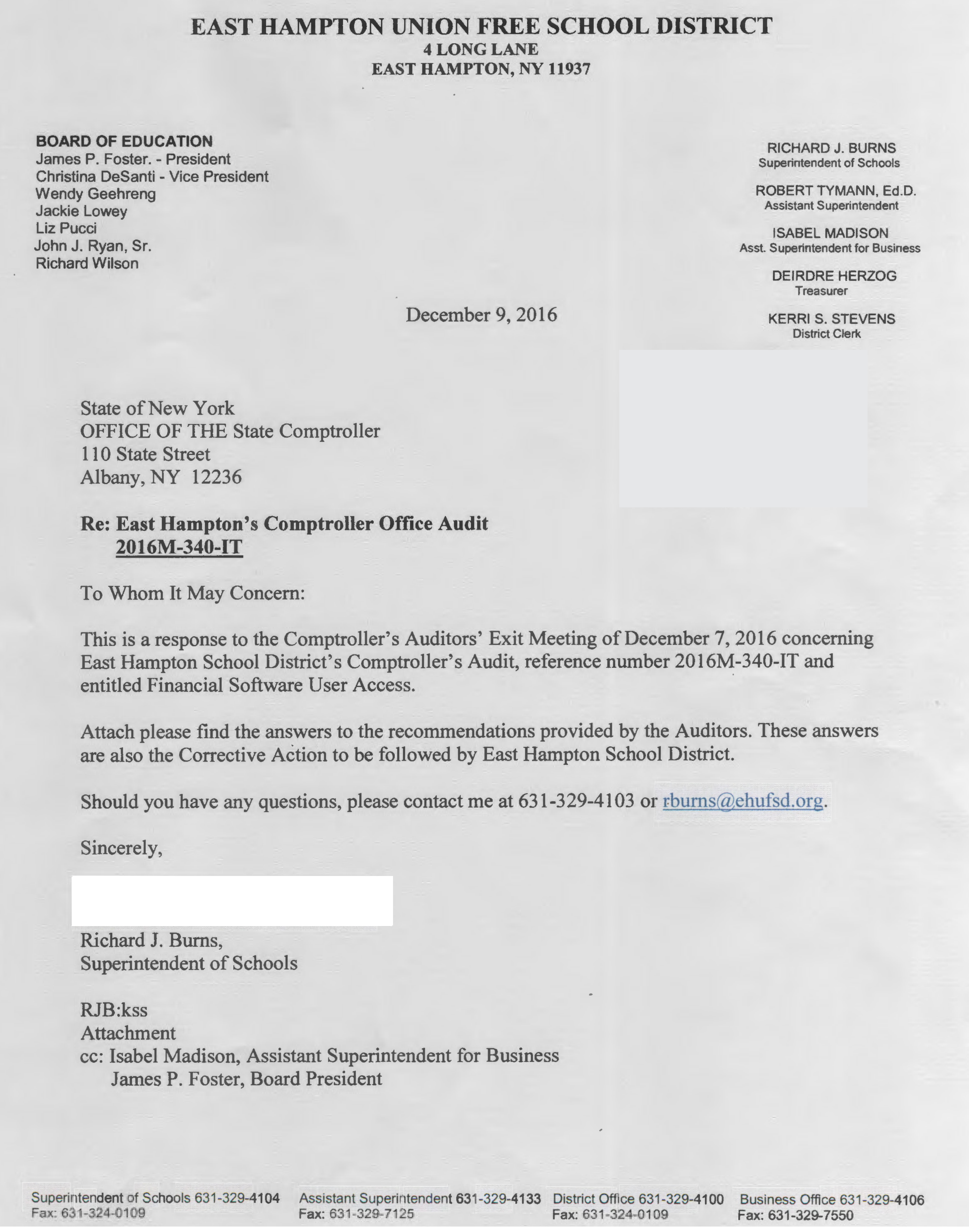
5. Routinely generate and review financial software audit logs and change reports to monitor user activity and compliance with computer use policies, provide the Assistant Superintendent for Business with user change reports monthly and provide audit trails for system maintenance to the Board on a quarterly basis.

6. Review the access rights for existing users and limit users' access rights to only those functions needed to perform their job duties.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

The District officials' response to this audit can be found on the following pages.



EAST HAMPTON UNION FREE SCHOOL DISTRICT

4 LONG LANE
EAST HAMPTON, NY 11937

RICHARD J. BURNS
Superintendent of Schools

ROBERT TYMANN, Ed.D.
Assistant Superintendent

ISABEL MADISON
Asst. Superintendent for Business

DEIRDRE HERZOG
Treasurer

KERRI S. STEVENS
District Clerk

December 9, 2016

State of New York
OFFICE OF THE State Comptroller
110 State Street
Albany, NY 12236

Re: East Hampton's Comptroller Office Audit
2016M-340-IT

To Whom It May Concern:

This is a response to the Comptroller's Auditors' Exit Meeting of December 7, 2016 concerning East Hampton School District's Comptroller's Audit, reference number 2016M-340-IT and entitled Financial Software User Access.

Attach please find the answers to the recommendations provided by the Auditors. These answers are also the Corrective Action to be followed by East Hampton School District.

Should you have any questions, please contact me at 631-329-4103 or rburns@ehufsd.org.

Sincerely,

[redacted]

Richard J. Burns,
Superintendent of Schools

RJB:kss
Attachment
cc: Isabel Madison, Assistant Superintendent for Business
James P. Foster, Board President

Financial Software User Access

District officials did not comply with the Board's computer control policy. The Board has not annually designated a system administrator. Instead, the Board annually appoints a Network Systems Manager who performs these duties. As a result, there may be confusion as to who is responsible for financial software administration. Also, the District does not have procedures outlining how user access rights should be established or modified and permissions are not reviewed quarterly to ensure a proper segregation of duties. Further, change reports are not provided to the Assistant Superintendent for Business monthly and audit trails are not reviewed and/or provided to the Board.

The Board adopted a computer control policy[1] that establishes procedures for granting access rights to the financial software. A system administrator is designated by the Board each year. The system administrator reports to the Assistant Superintendent for Business and has authority to change user account permissions and account code access for all user accounts on the financial software. The system administrator, with written approval of the Assistant Superintendent for Business, is responsible for creating, maintaining, managing permissions and removing user accounts as directed by the Assistant Superintendent for Business. The system administrator should maintain backup documentation of all user account creations and modifications and provide the Assistant Superintendent for Business with user change reports monthly. User permissions are required to be granted based on job duties and proper segregation of duties. The Assistant Superintendent for Business and system administrator are required to review permissions quarterly to ensure a proper segregation of duties and report to the Board. Finally, audit trails for system maintenance are required to be provided to the Board quarterly.

District officials did not comply with the Board's computer control policy. The Board has not annually designated a system administrator. Instead, the Board annually appoints a Network Systems Manager who performs these duties. As a result, there may be confusion as to who is responsible for financial software administration. Also, the District does not have procedures outlining how user access rights should be established or modified and permissions are not reviewed quarterly to ensure a proper segregation of duties. Further, change reports are not provided to the Assistant Superintendent for Business monthly and audit trails are not reviewed and/or provided to the Board.

We looked at all fifty users of the District's financial software and found that three users, including the Assistant Superintendent for Business, were granted system administrator access even though it was not required to perform their job duties. Also, District officials provided leave record, vendor record, budget transfer and personal private and sensitive information access rights to 18[2] users that did not require it to perform their job duties. Finally, District officials do not review audit logs and change reports or provide audit trails to the Board on a quarterly basis.

System Administrators — An individual who has financial system administrative rights can add new users, configure certain system settings, override management controls, create and change user access rights, and record and adjust entries. Accordingly, the financial system administrator should not be involved in financial operations. If this is not feasible, then system activity should be periodically reviewed, and audit logs should be generated and reviewed on a regular basis.

The Network Systems Manager and four other users were granted financial system administrator rights, including the Eastern Suffolk Board of Cooperative Education System (ESBOCES), the Assistant Superintendent for Business, the software vendor and the Director of Learning Technology and Instruction.

The Network Systems Manager required this access to manage the system and District officials told us that ESBOCES required this access to back-up the financial data on a daily basis. However, the Assistant Superintendent for Business, the software vendor and the Director of Learning Technology and Instruction did not need system administration access.

District officials told us that the Assistant Superintendent for Business was granted system administration rights when the District was notified of our audit. The Assistant Superintendent for Business needed the access to send the data requested by our Office but was not removed as system administrator after the data had been sent. With administrative rights, the Assistant Superintendent has the ability to add, delete and modify records in all functions of the financial software. In addition, she can grant user access, override controls and make changes to the system that may enable her to make intentional or unintentional changes. When we brought this to the attention of District officials, they removed the Assistant Superintendent for Business as a system administrator.

District officials told us that the software vendor required administration rights when the financial software was upgraded in August 2014 to add users and help with implementation and to perform system updates and maintenance. District officials also told us that the Director of Learning Technology and Instruction was the back-up to the Network Systems Manager and helped with resolving problems when the upgrade was implemented. Because some users may require access for only a limited time, District officials should review administration access and determine who needs administrative rights on a regular basis.

We also determined that no one maintains backup documentation of user account creations and modifications, routinely generates and reviews financial software audit logs and change reports to monitor user activity and compliance with computer use policies. Additionally no one provides the Assistant Superintendent for Business with user change reports monthly or audit trails for system maintenance to the Board on a quarterly basis.

We reviewed the audit trail for system administration transactions and found the ESBOCES and the Assistant Superintendent for Business did not add, delete or modify any users and that the Network Systems Manager, software vendor and the Director of Learning Technology did not inappropriately assign rights or users. Although we did not find any inappropriate system administration transactions, this type of access could allow users to make unauthorized changes to the accounting records, financial software security settings and user access rights. Therefore, the District should limit the number of system administrators to those who need it to perform their job duties.

Leave Records — Fourteen users, including the software vendor, can add, delete or modify leave records in the financial software. Each of the District's three school buildings and the Business Office has a designated individual who maintains the leave records for the building. There are backup employees for each of the individuals in the event that they are on vacation or otherwise unavailable. However, there are an additional five individuals who have access to add, delete or modify leave records. Because they are not responsible for entering leave records, these individuals do not need this access to perform their job duties. Employees who require this access to perform their job duties should not be allowed to enter, modify or delete information for their own leave time records.

We reviewed the leave records and accruals for 15[3] employees to determine if leave used was properly deducted from their leave accruals. We found minor errors with four of the employees' leave accruals. For example, two employees deleted a vacation day used from their own leave time records. Although we later determined that these leave days were used on a District holiday, these individuals should not have been able to delete information from their own leave time records. By allowing access to District leave records, there is an increased the risk of unauthorized modifications, deletions or additions to time records and individuals could use or be paid for leave time for which they are not entitled.

Vendor Records — Seven District employees can add, delete or modify purchase orders and vendor information. However, only two users, the Secretary to the Assistant Superintendent for Business and the Assistant Superintendent for Business need access to purchase orders and vendor information to perform their job duties. We reviewed 135 claims totaling $584,262 to confirm the ordering and shipping addresses were the District's address, vendor names and addresses were consistent throughout and that purchases were for valid expenditures. Although we found no discrepancies, this type of access could allow users to create fictitious vendors and issue purchase orders to those vendors for personal goods and services.

We also reviewed audit trails for nine[4] District employees. Seven users made no changes to vendor information, one user changed a phone number, and another user added 20 vendors during the audit period. Although the change to one vendor and addition of 20 vendors was appropriate, by allowing excess user access to vendor records District officials increase the risk that that fictitious vendors could be added or vendor records inappropriately changed, resulting in inappropriate payments. District officials told us the individual who added vendors required access because she was a backup to the employee who was responsible for adding vendors. After we brought this to the attention of District officials, they removed her permissions because she no longer required access to add vendors.

Budget Transfers — Nine users, including the software vendor, can add, delete or modify budget transfers. However, only two users, the Senior Clerk and the Assistant Superintendent for Business, needed access to budget transfers in the financial software to perform their job duties. Allowing users who do not need access to budget transfers increases the risk that budget transfers could be made without proper authorization and approval. We reviewed transfers for December 2014 and September 2015[5] and found the Senior Clerk made 16 transfers totaling $1,747,966. All 16 transfers were properly authorized and approved by the Assistant Superintendent for Business.

We also reviewed audit trails for the seven users who did not need access to budget transfer transactions to perform their job duties. One user (the Treasurer) made three budget transfers on August 22, 2015. The Assistant Superintendent for Business stated that these transfers were done as part of year-end procedures and that the Treasurer is her backup to do year-end journal entries. Therefore, according to District officials, three of the nine individuals need access to budget transfers on a regular basis. However, because the Treasurer does not require this access year round, it should be removed and restored for only as long as she needs it to do year-end journal entries. Allowing excess users the ability to make budget transfers increases the risk of unauthorized budget transfers resulting in expenditures exceeding what the Board intended.

Personal Private and Sensitive Information (PPSI) — PPSI is any information to which unauthorized access, disclosure, modification, destruction, or disruption of access or use could severely impact critical functions, employees, customers or third parties, or citizens of New York in general. Private information could include one or more of the following: social security number, driver's license number or non-driver ID, account number, credit card number, or debit card number and security code, or access code/password that permits access to an individual's financial account or protected student records. The ability to access PPSI should be limited to those employees who need access to perform their job duties.

Seven users had access to view employees' entire social security numbers. District officials explained that it was necessary for two users to have access to view the entire social security numbers to perform their job duties. Therefore, five users did not require this access. Allowing access to sensitive District data increases the risk that PPSI may be lost or compromised.

The District transitioned to new financial software during the summer of 2014. The first day the new system was used was September 3, 2014. District officials told us that they had encountered problems with restricting user permissions when transitioning to the new financial software. They told us that when they attempted to restrict access to permissions that were not related to users' job duties the users were unable to access permissions to areas in which they needed access to for their job duties.

Due to the improper assignment of system administrative rights and access rights for leave records, vendor information, budget transfers and PPSI and the lack of review of logs, change reports and audit trails, there is an increased risk that unauthorized changes to the accounting records, software security settings and user authorization privileges could occur and go undetected. This could lead to the loss or exposure of important financial data and cause interruptions to District operations.

Recommendation

1. **The Board should:**
   Annually designate and administrator for the financial software to clarify who is responsible for financial software administration.

   Following the recommendation of the auditors, the computer control policy will be amended; the Board of Education will be appointing an administrator to be in charge of the financial software at the annual Reorganizational meeting.

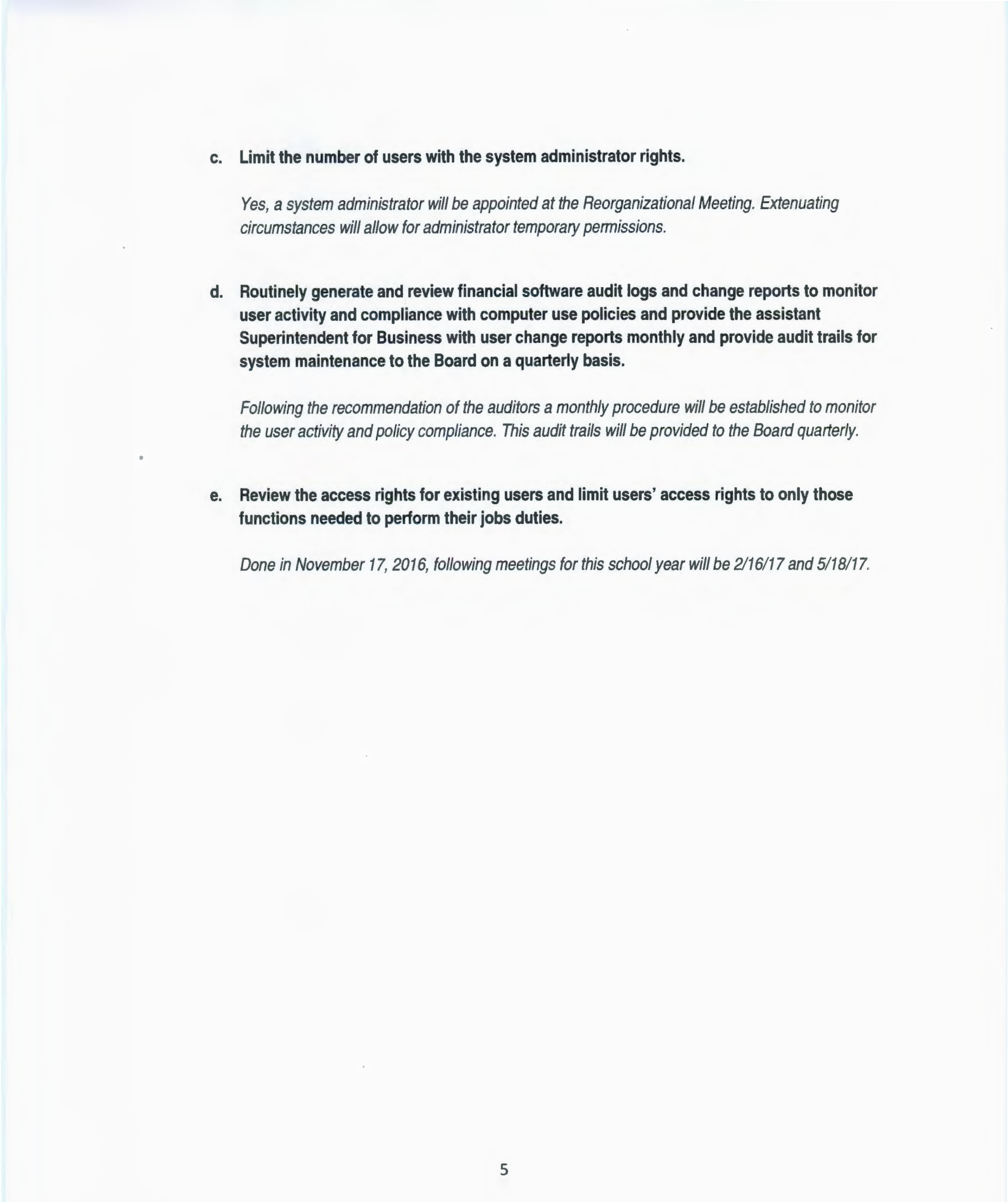
Recommendations

2. **District officials should:**
   a. **Develop written procedures outlining how user access rights should be established or modified based on job duties and proper segregation of duties.**

      The District started the correction of employee's permissions during the audit; according to the functions of the employees permissions are granted. The requests and approvals are filed. This procedure will be part of the amendment to the computer control police.

   b. **Review permissions to ensure a proper segregation of duties and report to the Board on a quarterly basis.**

      As per the recommendation of the Comptroller's Auditors, the administration has established a procedure where quarterly the IT department meets with Assistant Superintendent for Business, permissions and other audit functions are checked and corrections are done if needed. The first meeting happens on 11/17/16, we have scheduled the following for the rest of the year 2/16/17, 5/18/17.



c. **Limit the number of users with the system administrator rights.**

Yes, a system administrator will be appointed at the Reorganizational Meeting. Extenuating circumstances will allow for administrator temporary permissions.

d. **Routinely generate and review financial software audit logs and change reports to monitor user activity and compliance with computer use policies and provide the assistant Superintendent for Business with user change reports monthly and provide audit trails for system maintenance to the Board on a quarterly basis.**

Following the recommendation of the auditors a monthly procedure will be established to monitor the user activity and policy compliance. This audit trails will be provided to the Board quarterly.

e. **Review the access rights for existing users and limit users' access rights to only those functions needed to perform their jobs duties.**

Done in November 17, 2016, following meetings for this school year will be 2/16/17 and 5/18/17.

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

To achieve our audit objective and obtain valid evidence, we performed the following procedures:

- We interviewed officials and employees and reviewed policies and procedures to gain an understanding of user access to the financial software.

- We obtained all user access reports from the financial software.

- We reviewed user access permission reports for all 50 users of the financial software from September 1, 2014 through March 31, 2016 to determine the permissions each user had and compared them to their job descriptions.

- We reviewed the audit trails for individuals who had excessive user rights in the financial software as per the permission reports.

- We reviewed the audit trails for all transactions performed by the software vendor for the audit period.

- We reviewed the activity for all 13 employees who had access to attendance records in the financial software and the two employees who had administrative rights. We obtained from the software the date hired, job title and attendance records. We obtained attendance notices for the initial balances and the annual amounts accrued. We determined if the balances as of July 1, 2015 matched the ending balances for the prior fiscal year. We determined if days accrued were allowed by collective bargaining agreements or personal contracts. We determined if the days requested on request forms were entered into the financial software. For any discrepancies in days, we printed an audit trail for the individuals to determine if dates were deleted by the employees. We interviewed the human resources clerk regarding all discrepancies.

- We randomly selected two months, December 2014 and September 2015, one from each fiscal year during our audit period to review claims. The sample size decreased by choosing the median date that checks were printed in both months: December 12, 2014 and September 11, 2015. We selected all claims paid by checks printed on those two days. We reviewed the requisitions, purchase orders, invoices, packing slips, check stubs and the copies of the checks on the bank statements to determine if the ordering and shipping addresses were the District's address. We also determined if there were changes in any of the documentation related to addresses or vendor names and if the purchases were for valid expenditures. We also reviewed vendor address and vendor name change reports for any unusual changes.

- We randomly selected December 2014 and September 2015 as the sample months to be reviewed for budget transfers. We reviewed budget transfer documentation to determine if the proper signatures were acquired and if the vendors, where applicable, were legitimate District vendors. We compared totals against the financial system reports to determine if all budget transfers were properly accounted for.

- We reviewed the user administration audit analysis report to determine if users had access to view social security numbers.

We conducted this performance audit in accordance with 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.

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX D

OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE
Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

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

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

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

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence Counties

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313