



# North Rose-Wolcott Central School District

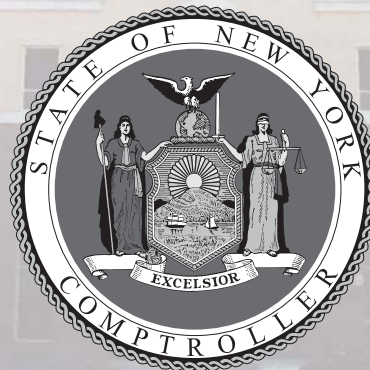
## Internal Controls Over Selected Financial Transactions

Report of Examination

Period Covered:

July 1, 2006 — December 11, 2007

2008M-34



Thomas P. DiNapoli

# Table of Contents

	<b>Page</b>
<b>AUTHORITY LETTER</b>	3
<b>EXECUTIVE SUMMARY</b>	5
<b>INTRODUCTION</b>	7
Background	7
Objective	7
Scope and Methodology	8
Comments of District Officials and Corrective Action	8
<b>SEGREGATION OF DUTIES</b>	9
Recommendations	11
<b>COMPUTERIZED FINANCIAL SYSTEM</b>	12
Recommendations	16
<b>APPENDIX A</b> Response From District Officials	17
<b>APPENDIX B</b> Audit Methodology and Standards	19
<b>APPENDIX C</b> How to Obtain Additional Copies of the Report	21
<b>APPENDIX D</b> Local Regional Office Listing	22

# State of New York Office of the State Comptroller

---

---

## **Division of Local Government and School Accountability**

June 2008

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 districts' 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 North Rose-Wolcott Central School District, entitled Internal Controls Over Selected Financial Transactions. 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 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*



## State of New York Office of the State Comptroller

---

# EXECUTIVE SUMMARY

The North Rose-Wolcott Central School District (District) is governed by the Board of Education (Board) which comprises nine elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer of the District and is responsible, along with other administrative staff, for the day-to-day management of the District under the direction of the Board.

The payroll supervisor processes payroll for an average of 400 employees every other week. The payroll supervisor reconciles the payroll account and the School Business Administrator certifies the payroll. During the audit period the Treasurer was responsible for recording receipts; transferring funds between and from District accounts; signing checks; and preparing and entering journal entries, with limited or no review. In addition, the Treasurer receives bank statements and cancelled checks, and reconciles each of the District's 41 bank accounts. The information technology (IT) department comprises a District technology coordinator. Wayne-Finger Lakes Board of Cooperative Educational Services (BOCES) provides part-time technicians and Monroe #1 BOCES administers the financial application.

### **Scope and Objective**

The objective of our audit was to assess the District's internal controls over selected financial activities and information technology for the period July 1, 2006 to December 11, 2007. Our audit addressed the following related questions:

- Are internal controls over selected financial activities appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over information technology systems appropriately designed to adequately safeguard District assets?

### **Audit Results**

Payroll duties are not properly segregated and compensating controls are inadequate. The payroll supervisor has the ability to create new employee records, update employee information, input/update salary detail, process payroll, and print and distribute payroll checks for the District. As a result, the payroll function is at a heightened risk for payroll errors and irregularities to occur and go undetected.

The District has not adequately segregated the duties of the Treasurer. The Treasurer is responsible for recording receipts; transferring funds between and from District accounts; signing checks; and preparing and entering journal entries. In addition, the Treasurer receives bank statements and cancelled checks and prepares the Treasurer's Report for the Board. However, the Treasurer has not performed timely bank reconciliations and all of the Treasurer's duties are performed with little or no oversight or review. As a result, there is an increased risk that errors could occur and not be detected in a timely manner, which could result in the misuse and loss of District assets.

Management has not protected District assets by ensuring that the administration of the computerized financial management system was properly assigned to someone outside of the Business Office. Two users tested had inappropriate levels of access in the financial software system. Additionally activity audit logs are not reviewed by management. The Board has not adopted policies and procedures to address information technology (IT) concerns. These concerns encompass: the type of confidential and sensitive information that users of the financial system should have access to, personal uses of District computer resources, timely system and security updates for District notebook computers, the security of the Districts IT assets, including servers, and disastrous events that may result in the loss of critical functions and/or data.

### **Comments of District Officials**

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 plan to initiate corrective action.

# Introduction

## Background

The North Rose-Wolcott Central School District (District) is located in the Towns of Butler, Huron, Lyons, Rose, Savannah, Sodus and Wolcott in Wayne County. The District is governed by the Board of Education (Board) which comprises nine elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer of the District and is responsible, along with other administrative staff, for the day-to-day management of the District under the direction of the Board.

There are four schools in operation within the District, with approximately 1,500 students and 400 employees. The District's budgeted expenditures for the 2007-08 fiscal year are \$24 million, which are funded primarily with State aid, real property taxes, and grants.

The payroll supervisor processes payroll for over 400 employees every other week. The payroll supervisor reconciles the payroll account and the School Business Administrator certifies the payroll. During the audit period the Treasurer was responsible for recording receipts; transferring funds between and from District accounts; signing checks; and preparing and entering journal entries, with limited or no review. In addition, the Treasurer receives bank statements and cancelled checks and reconciles each of the District's 41 bank accounts with little or no oversight or review. The information technology (IT) department comprises a District technology coordinator. Wayne-Finger Lakes Board of Cooperative Educational Services (BOCES) provides part-time technicians and Monroe #1 BOCES administers the financial application.

## Objective

The objective of our audit was to assess the District's internal controls over selected financial activities and information technology. Our audit addressed the following related questions:

- Are internal controls over selected financial activities appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over the information technology systems appropriately designed to adequately safeguard District assets?

**Scope and  
Methodology**

We examined internal controls over selected financial activities and the information technology systems of the District for the period July 1, 2006 to December 11, 2007.

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.

**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 plan to initiate corrective action.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the General Municipal Law, Section 2116-a (3) (c) of the Education Law and Section 170.12 of the Regulations of the Commissioner of Education, the Board must approve a corrective action plan that addresses the findings in this report, forward the plan to our office within 90 days, forward a copy of the plan to the Commissioner of Education, and make the plan available for public review in the District Clerk's office. For guidance in preparing the plan of action, the Board should refer to applicable sections in the publication issued by the Office of the State Comptroller entitled *Local Government Management Guide*.

## Segregation of Duties

An effective system of internal controls provides for positions that are compatible, and allows for adequate segregation of duties thus reducing the risk of errors and irregularities. This is done by ensuring that no single individual has control over all phases of a transaction: authorization, custody, and record keeping. When it is not practical to segregate duties because of limited staff resources, it is important for the Board to establish compensating controls.

The District had not adequately segregated the duties of the Treasurer and the payroll supervisor. In addition, bank reconciliations are not being performed in a timely manner.

Payroll Supervisor — Internal controls for payroll normally consist of written policies and procedures that describe employee responsibilities in preparing and disbursing payroll. Another feature of a good system of internal controls over payroll processing requires proper segregation of duties so that no one employee performs most or all of the three key payroll duties of authorization (e.g., adding employees to the payroll), recordkeeping (e.g., entering transactions that affect gross pay amounts) and asset custody (e.g., signing checks or distributing signed checks.) When adequate segregation of payroll duties is not feasible, management can implement mitigating controls to limit the risk of errors or irregularities. Mitigating controls include having someone independent of the payroll process examine computer-generated payroll exception reports for specific activities (such as payroll additions or gross pay changes) or review audit logs that monitor payroll system activity for unusual transactions or adjustments. The institution of mitigating controls in conjunction with specific policies and procedures are critically important when there is poor segregation of duties.

The Board has not established formal policies and District management has not developed procedures describing employee responsibilities for the processing of payroll. As a result, the payroll supervisor has the ability to create new employee records, update employee information, input/update salary detail and process payroll. The payroll supervisor then obtains the signature disk from the Treasurer and (unsupervised by the Treasurer) prints and distributes payroll checks for the District. Although, as a mitigating control, the claims auditor currently reviews the accuracy of new employees or modifications to current employees, it is not a formalized process that uses exception reports. This mitigating control, as presently implemented, is not sufficient to limit the risk of errors or irregularities occurring.

We selected all employees from District payroll records to verify that they were indeed employees of the District. In addition, we tested the accuracy of 10 employees' and key officials' salaries. Our testing did not reveal any material exceptions.

The lack of segregation of duties without mitigating controls in place puts the District at risk of fraud, abuse, and professional misconduct through unauthorized payroll disbursements.

Treasurer — The District has not adequately segregated the duties of the Treasurer. Specifically, the Treasurer is responsible for performing bank reconciliations and, at the same time, is also responsible for the recording of receipts; transferring funds between and from District accounts; signing checks; and preparing, approving and reviewing journal entries. In addition, the Treasurer receives bank statements and cancelled checks and prepares the Treasurer's Report for the Board, which consists of reconciliations for each of the District's 41 bank accounts. All of the Treasurer's duties are performed with little or no oversight or review. The lack of segregation of duties in these areas increases the risk that errors could occur and not be detected which could result in the misuse and loss of District assets.

Because of this lack of segregation and oversight, we judgmentally selected samples of cash transactions from our audit period to determine whether cash was recorded and accounted for properly. For example we reviewed 10 wire transfers, three bank reconciliations, 10 days of cash receipts, and 10 payments from warrant, to voucher, and then to the accompanying cancelled check. We found no discrepancies in the cash transactions tested.

Bank Reconciliations — The timely reconciliation of bank account balances to general ledger cash balances is essential. This process must provide for the timely identification and documentation of differences between the District's book balances and the bank's cash balances. Ideally, an employee that is independent of the cash custody and record-keeping functions of the District would perform bank reconciliations. Once completed, the bank reconciliations must be submitted to the Board, or its designee, such as the claims auditor or audit committee, for review. Bank reconciliations provide a unique opportunity for an internal verification of cash receipt and disbursement transactions.

The Board is provided with a Treasurer's Report on a monthly basis. This report is prepared by the Treasurer, and is not reviewed or approved by another employee prior to submission to the Board. The Treasurer's Report includes the bank reconciliations for the District's 41 bank accounts. We reviewed three general fund checking account

reconciliations to determine if they were done correctly and timely. We reviewed July 2006, February 2007, and June 2007. The July 2006 reconciliation was presented to the Board in December 2006, the February reconciliation in May 2007 and the June reconciliation was presented in December 2007. Generally bank reconciliations should be completed within a month after receiving the bank statement. Without timely bank reconciliations, performed and reviewed by an individual independent of the cash custody function, District officials cannot be assured the accounting records are correct or that monies are accounted for properly. While the bank reconciliations were not completed in a timely manner, our testing did not disclose any errors in the performance of the bank reconciliations.

## **Recommendations**

1. District officials should evaluate the payroll supervisor's and Treasurer's duties and responsibilities and assign them to other Business Office staff to better segregate duties.
2. The District should select an employee independent from the payroll department, such as the claims auditor, to periodically distribute payroll checks to verify the existence of employees.
3. District management should require complete, accurate, and timely bank reconciliations within a month after the District has received the bank statement.

## Computerized Financial System

The District uses a computerized financial system, which presents a number of internal control risks that must be addressed, including unauthorized access to data, unauthorized changes to data and the potential loss of data. Access rights must be assigned based upon job function and incompatible duties must be separated. Administrative rights must not be granted to someone responsible for significant business functions and management approval must be required to change user access. Policies and procedures establish the administration of the system including the approval levels required for individual users and the level of access to confidential and sensitive information granted to users of the financial system. Additionally general IT policies and procedures would prohibit most personal uses of District computer resources, require notebook computers to be periodically brought into and connected to the District server for software updates, and limit District server access to only authorized persons to protect data from loss. The policy should also provide for Management review of activity audit logs to provide a mechanism for individual accountability, reconstructing events and problem monitoring. Finally a formal disaster plan is necessary to provide guidance on the prevention of loss of computer data in the event of a disaster.

Control Over User Rights — To ensure proper segregation of duties and internal controls, the computer system must only allow users access to the functions necessary to fulfill their job responsibilities. Access controls prevent users from being involved in multiple aspects of financial transactions. Generally, a system administrator is designated as the person who has oversight and control of the system, and the ability to add new users as well as change users' passwords and access. With this ability, administrators are able to control and use all aspects of the software. A good system of controls requires the separation of this position from the Business Office function.

The Deputy Treasurer / secretary to the School Business Administrator holds the incompatible position of system administrator. As Deputy Treasurer / secretary to the School Business Administrator, she is responsible for significant business functions. As the system administrator, she has access to the administrative module.<sup>1</sup> This

<sup>1</sup> A module is a subsystem for a particular business function. The administrative module allows the user to set the access rights for other modules (including among others purchasing, revenue, general ledger, payroll, etc.), add new users, delete users, and perform basic system administrative tasks without management approval or an audit trail.

ability to control access rights (especially her own) and perform financial operations increases the risk of fraud, waste, abuse, or significant system errors.

We also found that access was not restricted to only those modules that were required by individual employee job descriptions and / or official duties. For example, we found that the Treasurer had access to all modules except benefits and the Substitute Treasurer, who succeeded the Treasurer effective January 1, 2008, had full access to all modules except benefits and human resources. Due to this improper segregation of duties, there was increased financial risk to the District.

Audit Logs — A computerized financial system provides a means of determining, on a constant basis, the identity of the individual accessing the system and the type of transactions that were processed. Audit logs maintain a record of activity by system or application process. The audit log provides information such as the identity of each person who has accessed the system; the time and date of the access; what activity occurred; and the time and date of logoff. Management, or Management’s designee, would review this audit log to monitor the activity of users who access the financial software. This tool provides a mechanism for individual accountability, reconstructing events and problem monitoring. However, Management’s ability to detect and properly address unauthorized activities was limited because they did not review the audit logs available.

Staff Use of Computerized Information Resources — To help protect the District’s computing environment, the Board adopted a policy and regulation entitled “Staff Use of Computerized Information Resources.” This guidance is especially important as every teacher in the District (approximately 160) is provided with a notebook computer, which they are allowed to freely move and use. This includes taking the computer home over the summer. The regulation states, in part, that engaging in practices that threaten the District’s computer system (DCS) (e.g., loading files that may introduce a virus) or using unauthorized software on the DCS are prohibited. The District’s policy and regulation are deficient in several respects.

First, the District’s policies do not prohibit most uses of District computers for personal purposes. As a rule, District-owned resources, such as computers, must be used primarily in furtherance of District purposes. We recognize that, like the use of a telephone, occasionally it may be necessary for District personnel to use computers, e-mail, or an internet connection during the business day for personal matters such as family care, transportation, weather or changes in the employee’s work schedule, etc. Nonetheless, District personnel must

keep the frequency and duration of such occasional personal use to a minimum. When personal use is more than incidental and occasional, it interferes with an employee's job performance or productivity.

An additional concern of the personal use of notebook computers is the ability of teachers to freely download or install programs while connected from home. Although the District has content filters on its network servers to block internet access to certain objectionable websites, chat rooms and free e-mail accounts, the filters only work when the internet is accessed through the District's network. The filters do not work when the internet is accessed in any other manner, such as when an individual uses a notebook computer to access the internet from his or her home. A best practice would be for the District's policy to explicitly prohibit use of District computer resources for most personal purposes and describe the limited circumstances when occasional personal use is permissible. It would also be prudent to take measures to more fully protect District technology assets, such as installing content filters and firewalls on the individual notebook computers, especially if the District continues to allow teachers the ability to access the internet through a non-District network and install personal programs. Another prudent procedure would be a periodic review of the notebooks by management to assure that the notebook has been used in conformance with District policy.

A second weakness with the District's policy and regulation is that it does not ensure critical operating system and security updates (including the antivirus programs) are updated timely on the teachers' notebook computers. Updates on teachers' notebook computers are automatically provided when a teacher logs into the District network. The concern here however is that teachers' notebook computers are taken home, used, and kept at home and not brought into the school to receive these updates on a regular basis. This possibility, along with the weakness of not prohibiting most personal use of the notebook computer, could create a situation in which a virus-laden notebook computer is connected to the District's network, and spreads the virus District-wide. The District policy must require notebook computers to log onto the network on a regular basis in order to keep security programs up to date.

Access to Personal Information — Maintaining adequate security over sensitive personal data helps to ensure that individuals are protected from loss and malicious misuse. Sensitive personal data can include items such as medical information and Social Security numbers. In the Districts financial system, we found that 15 out of 26 users have "default to view" access to sensitive personal information for District employees. This was caused by the default settings in the financial system never being modified after installation was first

completed. The effect is that inappropriate or malicious users of the financial system could use an individual's personal information for financial gain. We shared our concerns with District officials and they indicated that they would correct the problem.

Physical Access Controls Over Network Systems — An effective internal control system restricts physical access to the IT system, especially servers. The servers are assets the District must protect. Unrestricted access to the server room is dangerous to the security of the District's computer system. An individual could log into the network and thus into applications and could alter records or physically destroy the equipment. This could result in the District expending significant resources in both time and money to correct or repair data and equipment. Secure access would be enhanced by installing doors and keeping them locked at all times, controlling the keys, and documenting visitors' arrivals and departures. In addition, the server rooms must be located in an area that provides adequate ventilation. The Board has not established policies or procedures to ensure that the system's equipment is located in a secure location with adequate ventilation.

We inspected the District's IT equipment and found the network servers located in two District buildings. The first server was located in a community area where any number of individuals could have access; there is no door to lock the room where the server is located. The other server was located in a common area where five individuals work. The door was unlocked and the room was used to store coats and other items. In addition the District does not keep a log of who enters the server rooms. The two server rooms did not have temperature controls in place. Under the current conditions, it would be difficult for District officials to prevent unauthorized and/or malicious access to these assets or to identify the party responsible if such access did occur. In addition to the potential loss of costly equipment, server failures result in additional work for IT staff and a decrease in productivity for employees whose work is interrupted.

Disaster Recovery — An effective internal control system for information technology requires the adoption of a formal disaster recovery plan to prevent loss of computer equipment and data, and procedures for the recovery of data in the event of a loss. A disaster recovery plan (DRP) – Sometimes referred to as a business continuity plan (BCP) or business process contingency plan (BPCP) – describes how an organization is to deal with potential disasters. A plan consists of the precautions taken to minimize the effects of a disaster and to enable the organization to either maintain or quickly resume mission-critical functions. Typically, disaster recovery planning involves

an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention.

The Board has not established formal policies and procedures to address disastrous events that may result in the loss of critical functions and/or data. Therefore the District does not have a formal disaster recovery plan, and in the event of a catastrophic event, District personnel will have no written guidelines or plan to follow. This could result in the District losing critical equipment and/or data with no ability to recover functionality.

## **Recommendations**

4. District officials should ensure that the responsibility of setting user access rights is segregated from any user who has significant responsibilities within the Business Office.
5. District officials should monitor users access rights to ensure they are based on job functions and responsibilities, and promote proper segregation of duties.
6. District officials should review users' activities using audit logs.
7. The Board should revise its computerized information resources policy and regulation to address personal use of the Districts computer resources and to require teachers' notebook computers to be periodically connected to the District's network. Additionally all District employees should certify that they have read and understand the District policies and procedures regarding computer use.
8. The District should restrict access to sensitive personal information to employees and officials that utilize the information as part of their job duties. The District should develop a policy and implement procedures detailing who should have access to sensitive personal information in their financial system.
9. The Board should adopt policies and procedures to restrict physical access to its IT system. The policies should require the physical components of the IT system to be located in an area protected from unauthorized access and adequately ventilated.
10. The Board should adopt a formal disaster recovery plan.

## **APPENDIX A**

### **RESPONSE FROM DISTRICT OFFICIALS**

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



Cougars

# NORTH ROSE - WOLCOTT CENTRAL SCHOOL DISTRICT

11669 SALTER-COLVIN ROAD, WOLCOTT, NEW YORK 14590 FAX (315) 594-2352

Lucinda Miner  
Superintendent  
315.594.3141

Dr. John Boronkay  
Director of Curriculum  
315.594.3141

Robert D. Magin  
Business Administrator  
315.594.3150

Angela Kirkey  
Coordinator of Pupil Services  
315.587.9937 FAX 315.587.9925

May 8, 2008

[Redacted] of Local Government  
and School Accountability  
Office of the State Comptroller  
The Powers Building  
16 West Main Street-Suite 522  
Rochester, New York 14614

This letter is in response to your preliminary draft findings discussed with the North Rose-Wolcott Central School District on Wednesday, April 23, 2008.

1. The district acknowledges that we need to evaluate the duties and responsibilities of the payroll supervisor and the treasurer. While it is hard to have appropriate segregation of duties with a limited size staff, we will strive to address this concern.
2. Currently, the secretary to the school business administrator distributes payroll checks to verify the existence of employees and the accuracy of checks. We feel that this is an appropriate verification.
3. Complete, accurate and timely bank reconciliations are a priority for us. Since January 2008, we have been on schedule with bank reconciliations being completed within a month of receiving the bank statements.
4. Currently the secretary to the school business administrator has the responsibility of setting using access rights. We will review whether there is a more appropriate designee to take over this responsibility.
5. Proper segregation of duties is difficult with a small business office staff. The school business administrator will review duties and monitor user access rights.
6. The school business administrator will review users' activities using audit logs.
7. The board will review the district's current policy and regulations concerning the use of district computer resources. We will also be implementing a system for all district employees to certify that they have read and understand the policies and procedures.
8. The district will review which employees have access to sensitive personal information. Our goal is to ensure that it is restricted to employees that need this information as part of their job duties.
9. The board will review its policies and procedures in reference to the physical access to its IT system.
10. The board will work toward adopting a formal disaster recovery plan.

Sincerely,

Lucinda Miner  
Superintendent

LM:rm

## APPENDIX B

### AUDIT METHODOLOGY AND STANDARDS

Our overall goal was to assess the adequacy of the internal controls put in place by officials to safeguard District assets. To accomplish this, we performed an initial assessment of the internal controls so that we could design our audit to focus on those areas most at risk. Our initial assessment included evaluations of the following areas: financial oversight, cash receipts and disbursements, purchasing, payroll and personal services, and information technology (IT).

During the initial assessment, we interviewed appropriate District officials, performed limited tests of transactions and reviewed pertinent documents, such as District policies and procedures manuals, Board minutes, and financial records and reports. In addition, we obtained information directly from the computerized financial databases and then analyzed it electronically using computer-assisted techniques. This approach provided us with additional information about the District's financial transactions as recorded in its databases. Further, we reviewed the District's internal controls and procedures over the computerized financial databases to help ensure that the information produced by such systems was reliable.

After reviewing the information gathered during our initial assessment, we determined where weaknesses existed, and evaluated those weaknesses for the risk of potential fraud, theft and/or professional misconduct. We then decided upon the reported objectives and scope by selecting for audit those areas most at risk. We selected payroll, cash receipts and disbursements, and information technology for further audit testing.

We performed the following tests:

- Reviewed Board minutes and District policies and procedures
- Interviewed and observed District employees and officials to gain an understanding of procedures in place and the nature of internal controls
- Distributed paychecks to employees listed on the payroll
- Examined completed payrolls for signatures of appropriate District officials
- Tested payroll calculations, footings, and extensions
- Traced pay rates from payrolls to approved schedules, contracts, and other documentation
- Examined a judgmental sample of receipts from District records to ensure they were appropriately deposited. We examined the corresponding cash receipts to ensure that they were intact, for the correct amount, timely, and matched the bank deposit.
- Examined bank transfers to determine if they were appropriate, authorized, supported, and properly documented

- Reviewed financial records and bank statements to verify that bank reconciliations were timely and properly performed.

We conducted our 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## 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**

Steven J. Hancox, Deputy Comptroller  
John C. Traylor, Assistant Comptroller

**LOCAL REGIONAL OFFICE LISTING**

---

**BUFFALO REGIONAL OFFICE**

Robert Meller, Chief Examiner  
Office of the State Comptroller  
295 Main Street, Room 1050  
Buffalo, New York 14203-2510  
(716) 847-3647 Fax (716) 847-3643  
Email: [Muni-Buffalo@osc.state.ny.us](mailto:Muni-Buffalo@osc.state.ny.us)

Serving: Allegany, Cattaraugus, Chautauqua, Erie,  
Genesee, Niagara, Orleans, Wyoming 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](mailto:Muni-Rochester@osc.state.ny.us)

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

**SYRACUSE REGIONAL OFFICE**

Eugene A. Camp, 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](mailto:Muni-Syracuse@osc.state.ny.us)

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

**BINGHAMTON REGIONAL OFFICE**

Patrick Carbone, Chief Examiner  
Office of the State Comptroller  
State Office Building, Room 1702  
44 Hawley Street  
Binghamton, New York 13901-4417  
(607) 721-8306 Fax (607) 721-8313  
Email: [Muni-Binghamton@osc.state.ny.us](mailto:Muni-Binghamton@osc.state.ny.us)

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

**GLENS FALLS REGIONAL OFFICE**

Karl Smoczynski, 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](mailto:Muni-GlensFalls@osc.state.ny.us)

Serving: Clinton, Essex, Franklin, Fulton, Hamilton,  
Montgomery, Rensselaer, Saratoga, Warren, Washington  
counties

**ALBANY REGIONAL OFFICE**

Kenneth Madej, Chief Examiner  
Office of the State Comptroller  
22 Computer Drive West  
Albany, New York 12205-1695  
(518) 438-0093 Fax (518) 438-0367  
Email: [Muni-Albany@osc.state.ny.us](mailto:Muni-Albany@osc.state.ny.us)

Serving: Albany, Columbia, Dutchess, Greene,  
Schenectady, Ulster counties

**HAUPPAUGE REGIONAL OFFICE**

Jeffrey P. Leonard, Chief Examiner  
Office of the State Comptroller  
NYS Office Building, Room 3A10  
Veterans Memorial Highway  
Hauppauge, New York 11788-5533  
(631) 952-6534 Fax (631) 952-6530  
Email: [Muni-Hauppauge@osc.state.ny.us](mailto:Muni-Hauppauge@osc.state.ny.us)

Serving: Nassau, Suffolk counties

**NEWBURGH REGIONAL OFFICE**

Christopher Ellis, 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](mailto:Muni-Newburgh@osc.state.ny.us)

Serving: Orange, Putnam, Rockland, Westchester  
counties