



Eldred Central School District Internal Controls Over Cash Disbursements and Security of Computerized Data

Report of Examination

Period Covered:

July 1, 2005 — July 2, 2007

2008M-45



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	3
EXECUTIVE SUMMARY	5
INTRODUCTION	7
Background	7
Objective	7
Scope and Methodology	7
Comments of District Officials and Corrective Action	8
INTERNAL CONTROLS OVER CASH DISBURSEMENTS	9
Recommendation	10
SECURITY OF COMPUTERIZED DATA	11
Computer Data Backup	11
Disaster Recovery	12
Computer Use Policy	12
Administrator Rights	13
Recommendations	14
APPENDIX A Response From District Officials	15
APPENDIX B Audit Methodology and Standards	18
APPENDIX C How to Obtain Additional Copies of the Report	20
APPENDIX D Local Regional Office Listing	21

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 Eldred Central School District, entitled Internal Controls Over Cash Disbursements and Security of Computerized Data. 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 Eldred Central School District (District) is governed by the Board of Education (Board) which comprises five 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 District uses a networked computer system to process and store non-financial data. The Information Technology (IT) administrator oversees the network system. The District's Treasurer is responsible for managing its finance-related operations. The Treasurer's office has its own separate computer system used to process the District's financial data.

Scope and Objective

The objective of our audit was to examine internal controls over cash disbursements and computerized data and assets for the period of July 1, 2005 to July 2, 2007. Our audit addressed the following related questions:

- Did the Board assess risks inherent in the Treasurer's duties and institute controls necessary to ensure that District assets are safeguarded?
- Did the Board establish comprehensive policies and procedures addressing the safeguarding of computerized data and assets?

Audit Results

District officials have not effectively assessed risks inherent in the Treasurer's duties to ensure that District assets are safeguarded. The Treasurer has complete control over the cash disbursements process, and has the ability to sign checks, initiate wire transfers, make journal entries and reconcile District bank accounts. While our testing did not reveal any material discrepancies, District officials must segregate key financial duties, or at least increase oversight of the Treasurer's functions, to reduce the risk that future errors and/or irregularities might occur and go undetected and uncorrected in a timely manner.

Additionally, the Board has not adopted formal policies and procedures to adequately protect District systems and data. Specifically, the District had not developed formal procedures for backing up financial

data, a formal disaster recovery plan or a computer use policy for employees. We found that District financial data was not being backed up at a secure off-site location, which puts the District at risk of losing data or incurring significant data recovery costs. Further, because the Board has not adopted a formal disaster recovery plan, District personnel do not have guidelines to follow to help minimize the loss of computer data in the event of a disaster. In addition, while the Board has adopted a computer use policy, it had not implemented the policy as of the end of our fieldwork to ensure all District personnel are aware of acceptable use and security policies. We also found that the Treasurer has access rights that conflict with his day-to-day financial duties. The Treasurer, rather than the District's IT administrator, has administrator rights to the District's financial data system, which allows him to access all business functions, to create new users, to change users' passwords and access rights, and to perform management overrides. With administrator rights to the financial system, the Treasurer has the ability to make unauthorized payments or change financial data without detection. Although our audit tests did not identify any inappropriate financial transactions, District officials should correct these control weaknesses to safeguard District systems and 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 planned to initiate corrective action.

Introduction

Background

The Eldred Central School District (District) is located in the Towns of Highland, Lumberland and Tusten in Sullivan County and Town of Deerpark in Orange County. The District is governed by the Board of Education (Board) which comprises five 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 two schools in operation within the District, with approximately 706 students and 203 employees. The District's budgeted expenditures for the 2006-07 fiscal year were \$14.8 million, which were funded primarily with State aid, real property taxes, and grants.

The District also has a District Treasurer (Treasurer) who is responsible for managing its finance-related operations. Some of the Treasurer's duties include opening/closing bank accounts, signing checks, initiating bank wire transfers, making cash transfers between funds, and reconciling bank accounts.

The District uses a networked computer system to process and store non-financial data. It is supported by several servers located at the high school and one server at the elementary school. In addition, the Treasurer's office has its own separate computer system used to process the District's financial data. The Information Technology (IT) administrator oversees the network system.

Objective

The objective of our audit was to examine internal controls over cash disbursements and computerized data and assets. Our audit addressed the following related questions:

- Did the Board assess risks inherent in the Treasurer's duties and institute controls necessary to ensure that District assets are safeguarded?
- Did the Board establish comprehensive policies and procedures addressing the safeguarding of computerized data and assets?

Scope and Methodology

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. Based on that evaluation, we determined that controls appeared to be adequate and limited risk existed in most of the financial areas we reviewed. We did determine that risk existed in the cash disbursements and IT areas and, therefore, we examined internal controls over cash disbursements and security of computerized data for the period July 1, 2005 to July 2, 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 planned 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*.

Internal Controls Over Cash Disbursements

District officials have the responsibility to assess risks inherent in the Treasurer's duties to ensure that all cash disbursement transactions are properly accounted for. An effective component of any cash disbursement process is proper segregation of duties. Cash disbursement duties should be segregated and computer access should be based upon job responsibilities to ensure that no single individual controls all phases of a transaction. If it is not practicable to segregate the cash disbursement duties of the Treasurer adequately, District officials should implement compensating controls as an alternative. Some examples of compensating controls include having someone independent of the business office perform monthly bank reconciliations or review the monthly bank reconciliations prepared by the Treasurer, and/or having an independent person review cancelled check images, electronic bank wire transfers and journal entries.

District officials have not effectively assessed risks inherent in the Treasurer's duties to ensure that District assets are safeguarded. We found that the Board did not ensure that the duties performed by the Treasurer relating to cash disbursements were properly segregated, or establish sufficient compensating controls as an alternative. The Treasurer has complete control over the cash disbursements process. His duties include opening/closing bank accounts, signing checks, initiating bank wire transfers, preparing journal entries, and reconciling bank accounts. No one reviews or approves the Treasurer's work, including approving journal entries and bank transfers. The Treasurer processed approximately \$15.4 million in expenditures for the 2006-07 fiscal year.

Due to the lack of segregation of duties over the cash disbursements process, we reviewed 45 disbursements totaling \$149,722 from District bank statements to determine if such disbursements were proper District charges, agreed to accounting records and were adequately supported. In addition, we judgmentally selected 11 electronic wire transfers totaling \$1,724,950 for a 6-month period and traced them to the supporting documents to determine whether the payments were legitimate. The District also made 28 payments to District officials for reimbursement of mileage, tuition and lodging, out of which we judgmentally selected five totaling \$2,872, to verify that they were authorized, documented and legitimate District expenses. Furthermore, we performed tests to determine that bank reconciliations were accurate and prepared timely. While our testing did not reveal any material discrepancies, District officials must segregate key financial

duties, or at least increase oversight of the Treasurer's functions, to reduce the risk that future errors and/or irregularities might occur and go undetected and uncorrected in a timely manner.

Recommendation

1. District officials should provide for an adequate segregation of duties so that no one person controls all aspects of the cash disbursement process.

Security of Computerized Data

An effective system of internal controls over computerized data includes policies and procedures adopted by the Board to help minimize the loss or corruption of essential data. Those policies and procedures should address data back-up and disaster recovery. District officials should prepare a disaster recovery plan that details the responsibilities of individuals and the procedures to be followed to minimize business cycle interruption and address the process of returning to normal business functioning, with minimum lost data or productivity. Further, the Board should adopt computer use policies to define appropriate user behavior, and the tools and procedures necessary to protect information systems. Finally, to help reduce the risk of misuse and/or alteration of financial data, an employee outside of business office should have administrator rights to the IT system so that business office employees cannot grant themselves unauthorized access to District systems and data.

The Board has not established comprehensive policies and procedures addressing the safeguarding of computerized data and assets. Specifically, the Board has not adopted formal policies relating to computer data backup, a formal disaster recovery plan, or assignment of administrator's rights. While the Board has adopted a computer use policy, it had not implemented the policy as of the end of our fieldwork. The following represents more specific areas where the Board should enhance controls over safeguarding computer data.

Computer Data Backup

The Board should adopt policies and procedures to protect data from the risk of loss due to threats or disasters, and provide for the restoration of data should this occur. Data stored on computers and servers should be backed-up (a duplicate copy of information made) on a routine basis, and stored at a secure off-site location to minimize the risk of loss due to a disaster at the server location site.

The Board has not adopted formal policies addressing adequate backup of computer data. Furthermore, although District officials had procedures to back up their financial and non-financial data, they were deficient in that the tapes used to backup this data were not stored in a secure off-site location. Instead, non-financial data backups were stored in the same room as the server. As a result, backups of non-financial data were subject to the same risks as the original data, and the purpose of this control procedure was defeated. For example, a fire or some other catastrophe in the server room could have destroyed both the original data and the backup files. According to District officials,

backups of non-financial data are now being stored at secure offsite facility.

However, District officials told us financial data was not being backed up at a secure off-site location. Instead, backups of financial data are maintained by the Treasurer on a USB (“flash” or “jump”) drive which he takes home. The small size and portability of a USB drive increases risk that data on it may be lost or stolen. Because the financial data is located on a separate computer system from other District data, District officials did not include it when establishing the new off site storage procedures.

Disaster Recovery

The District’s internal control system over safeguarding computerized data should include a formal disaster recovery plan to address the possible loss of computer equipment and data and procedures for recovery in the event of such a loss. The plan should include precautions to be taken to minimize the effects of a disaster and enable the District to either maintain or quickly resume mission-critical functions. The plan may also include a significant focus on disaster prevention.

The Board has not established a formal disaster recovery plan to address potential disasters. Consequently, in the event of a disaster, District personnel have no guidelines or plan to follow to help minimize the loss of computer data or guidance on how to implement data recovery procedures. This could result in the District losing data or incurring significant data recovery costs.

Computer Use Policy

An adequate computer use policy defines the Board’s goals for the acceptable use of District equipment and establishes security measures to protect the District’s resources and confidential information. More specifically, the policy should include procedures governing acceptable use of technology including computers (including portable laptops), Internet, electronic-mail and portable devices;¹ information protection; virus protection and prevention; and penalties for violating these policies. Furthermore, computer use policies should be distributed to and acknowledged by a written understanding from all employees and students.

Although District officials require written acknowledgement of the computer use policy by students, District employees (including teachers) are not required to sign a computer use policy. The Board adopted a computer use policy for District employees in June 2007, but they have not implemented it. District officials told us their goal is to implement the computer use policy in the 2008-09 fiscal year.

¹ Portable devices include such items as personal digital assistants (PDAs); jump drives, also known as USB drives; flash drives; keychain drives; disk-on-keys; and MP3 players.

Because District employees are not required to sign the computer use policy, we sought to determine if the District's computers were being used appropriately. We examined 10 District laptop computers for evidence of inappropriate personal use. We found no significant evidence of inappropriate personal use on the computers we tested.

While comprehensive computer use policies do not guarantee the proper use of District computer assets, the lack of such policies significantly increases the risk that mission critical data, hardware and software systems may be lost or damaged or that inappropriate personal use of computers by staff could occur.

Administrator Rights

The Board should establish adequate internal controls over computerized data to protect systems and data from unauthorized access. To ensure that adequate internal controls exist over computerized data, users should only be allowed to access the computer functions necessary to fulfill their job responsibilities. Having proper access controls in place prevents 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 IT system, including the ability to add new users and change users' passwords and rights. With this ability, the administrator is able to control and use all aspects of the software. A good system of internal controls requires that the position of administrator for the financial software not be an employee of the business office. Ideally, the District's IT network administrator should also serve as the administrator for the financial software.

We found that the Treasurer is the only District employee with administrator rights to the District's financial data system. Administrator rights allow him to have access to all business functions within the financial data system. He was also responsible for creating new users, updating users' access rights, and performing other administrative functions, including management overrides. With administrator rights to the financial system, the Treasurer has the ability to make unauthorized payments or change financial data without detection. District officials indicated that the Treasurer had administrator rights in order to compensate for limited staff at the District.

Because of this weakness, and also because the Treasurer performs all the District's financial duties without oversight by any other District official, we tested three termination payments totaling \$81,711 and six payments for approved contracts totaling \$430,331 to determine if such disbursements were properly authorized, approved and calculated correctly. Although we found no exceptions with these payments, District officials should correct this control deficiency that allows the Treasurer access rights that conflict with his day-to-day job duties.

Recommendations

2. The Board should adopt comprehensive policies and procedures addressing the safeguarding of computerized data and assets including the securing of computer data backups at an off-site storage location.
3. The Board should adopt policies and procedures that require the establishment of a formal disaster recovery plan to address the range of threats to the District's information technology system.
4. The Board should implement and distribute a computer use policy to all District employees.
5. District officials should revoke administrator rights from the District Treasurer and give the rights to the District's IT network administrator.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

April 24, 2008

Attn: [REDACTED]
Binghamton Regional Office
Office of the State Comptroller
State Office Building Room 1702
44 Hawley Street
Binghamton, NY 13901-4417

Dear [REDACTED]

The Eldred Central School District Board of Education and administration have thoroughly reviewed the findings and recommendations of the recent examination of the district and respond to the recommendations as follows: -

Area of Review: Internal Controls Over Cash Disbursements

Recommendation 1: District officials should provide for an adequate segregation of duties so that no one person controls all aspects of the cash disbursement process.

Response: The district agrees with this recommendation. Budget constraints and size of the district impact this significantly. We plan to identify specific responsibilities that can be assigned to other district personnel to minimize the single person control over all aspects of the process. New personnel have been employed in other positions who have the skills necessary to facilitate these assignments. The superintendent will also be assigned specific responsibilities in order to improve oversight of the cash disbursement procedures. In addition, the district is participating in a discussion and study of the creation of a central business office with the Sullivan County BOCES which in theory allow us to move some of the business office functions to this entity in the future.

Area of Review: Security of computerized Data

Recommendation 2: The Board should adopt comprehensive policies and procedures addressing the safeguarding of computerized data and assets including the securing of computer data back ups at an off-site storage location.

Response: The Board agrees with this recommendation and will direct the superintendent to request sample policies and procedures in order to develop the requisite policies and procedures appropriate for the district.

Recommendation 3: The Board should adopt policies and procedures that require the establishment of a formal disaster recovery plan to address the range of threats to the District's information technology system.

Response: The Board agrees with this recommendation and will direct the superintendent to request sample policies and procedures in order to develop the requisite policies and procedures for establishment of a formal disaster recovery plan appropriate for the district's technology system. In addition, the district is part of a county wide grant proposal to fund the development of a comprehensive disaster recovery plan submitted in December 2007.

Recommendation 4: The Board should implement and distribute a computer use policy to all District employees.

Response: The Board agrees with this recommendation. All district employees were provided with a computer use agreement in February 2008

Recommendation 5: District officials should revoke administrator rights from the district treasurer and give the rights to the District's IT administrator.

Response: The District agrees with this recommendation and has revoked administrator rights from the district treasurer and reassigned those rights to the District's IT administrator effective May 1, 2008.

I trust that this meets the requirements of the response to the preliminary report.

Sincerely,



Robert Warden
President, Board of Education
Eldred Central School District

RW:br

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.

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. Based on that evaluation we determined that controls appeared to be adequate and limited risk existed in most of the financial areas we reviewed. We then decided upon the reported objective and scope by selecting for audit those areas most at risk. We selected cash disbursements and security of computerized data for further audit testing.

In order to accomplish the objective of this audit and to gain an understanding of how the business management system is used, become familiar with access and limitations, and to gain an understanding of what different controls exist and how the District functions, we:

- Reviewed current procedures relating to business office duties and roles regarding the District Treasurer
- Reviewed pertinent documents including: cancelled check images, bank statements, warrants, cash disbursements journals and various other accounting records and financial reports to determine if cash disbursement transactions were adequately supported, proper District charges, properly authorized and agreed to the accounting records
- Compared information included on cancelled check images with related supporting documentation for any unusual or improper payments to employees
- Reviewed bank reconciliations for accuracy, completeness and timeliness
- Reviewed electronic bank transfers for legitimacy, approval and accuracy
- Reviewed check number sequence used to ensure that all checks were properly accounted for

- Physically examined 10 computers to determine if only District related software was installed and that users had not viewed inappropriate websites
- Reviewed current procedures relating to computer data back up, disaster recovery, acceptable use and administrator's rights.

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-Bufferalo@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

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

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

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

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

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

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

Serving: Orange, Putnam, Rockland, Westchester
counties