



Tioga Central School District

Internal Controls Over Computer Data and Cash Disbursements

Report of Examination

Period Covered:

July 1, 2004 - December 5, 2005

2006M-64



ALAN G. HEVESI

Table of Contents

	Page
AUTHORITY LETTER	3
INTRODUCTION	5
Background	5
Objectives	5
Scope and Methodology	6
Comments of District Officials and Corrective Action	6
COMPUTER DATA SAFEGUARDS	7
Recommendations	9
CASH DISBURSEMENTS	10
APPENDIX A Response From District Officials	11
APPENDIX B OSC Comment to District Officials' Response	14
APPENDIX C Audit Methodology and Standards	15
APPENDIX D How to Obtain Additional Copies of the Report	17
APPENDIX E Local Regional Office Listing	18

State of New York Office of the State Comptroller

Division of Local Government Services and Economic Development

August 2006

Dear School District Officials:

One of the Office of the State Comptroller's top priorities is to identify areas where school districts can improve their operations and provide guidance and services that will assist school district officials in making those improvements. Further objectives are to develop and promote short-term and long-term strategies to enable and encourage school district officials to reduce costs, improve service delivery and to account for and protect their school districts' assets.

The reports issued by this Office are an important component in accomplishing these objectives. These reports are expected to be a resource and are designed to identify current and emerging fiscally related problems and provide recommendations for improvement. These reports also may identify positive aspects of school district operations that other school districts may wish to emulate. The following is our report on the Tioga Central School District — Internal Controls Over Computer Data and Cash Disbursements.

This audit was conducted pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article 3 of the General Municipal Law. The report contains opportunities for improvement for consideration by school district officials.

If we can be of assistance to you or if you have any questions concerning this report, please feel free to contact the local regional office for your county listed at the back of this report.

Respectfully submitted,

*Office of the State Comptroller
Division of Local Government Services
and Economic Development*

Introduction

Background

The Tioga Central School District (District) is located in the Towns of Barton, Candor, Nichols and Tioga in Tioga County. The District is governed by the Board of Education (Board) which comprises 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 (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 three schools in operation within the District, with approximately 1,221 students and 165 employees. The District's budgeted expenditures for the 2005-06 fiscal year are \$13.5 million, funded primarily with State aid, real property taxes and grants.

The District has two separate and distinct computer systems that process and store data, one for non-financial data such as student attendance and one for financial data. The non-financial data computer is located in one of the school buildings and is operated by District employees. The financial data computer is located in the District Business Office and is operated by other District staff. An independent contractor oversees the system.

The District internal claims auditor audits and approves all claims for payment. Business Office employees prepare cash disbursements transactions and send out checks to the appropriate vendors.

Objectives

The objective of our audit was to determine if internal controls over computer data safeguards and cash disbursements were appropriately designed and operating effectively to adequately safeguard district assets. Our audit addressed the following related questions:

- Has the Board established policies to ensure: data is stored on each computer in a climate controlled and secure area; computer data is properly backed up; and plans are in place to prevent or help address potential disasters to equipment and data?
- Has the Board established policies to monitor and control remote access to computer data?

- Are cash disbursements properly authorized and approved as well as recorded timely and accurately?

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: cash receipts and disbursements, purchasing, payroll and personal services, and capital assets and consumable inventories. 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 for computer data safeguards and cash disbursements and therefore, we examined the internal controls for these two areas for the period July 1, 2004 to December 5, 2005.

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 C 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. District officials also asked us to make some technical changes to our report and after considering them, we made appropriate revisions.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the General Municipal Law, the Board should prepare a plan of action that addresses the recommendations in this report and forward the plan to our office within 90 days. For guidance in preparing the plan of action, the Board may refer to applicable sections in the publication issued by the Office of the State Comptroller entitled *Local Government Management Guide*. We encourage the Board to make this plan available for public review in the District Clerk's office.

Computer Data Safeguards

One of the Board's managerial responsibilities is to design and implement a system of internal controls incorporating policies and procedures to provide reasonable assurance that all assets and resources entrusted to their care are used in accordance with all laws, regulations, policies and sound business practices as well as safeguarded against waste, loss, and misuse. Computer data is a valuable District resource. The District relies on computer data for making financial decisions and for reporting to State and Federal agencies. If the computers on which this data is stored fail, the results could range from inconvenient to catastrophic. Even small disruptions in electronic data systems can require extensive employee and consultant hours to evaluate and repair. Access to computer data systems should be controlled and monitored to reduce the risk of misuse and/or alteration of data resulting in potential financial loss to the District. Finally, a formal disaster plan is necessary to provide guidance on the prevention of the loss of computer data as well as the recovery of computer data in the event of a disaster.

The Board has not sufficiently addressed the safeguarding of computer data to ensure proper protection. Computer equipment and data are not protected from environmental factors and data is not properly backed up routinely. Additionally, the District has no formal disaster plan and there are no controls over remotely accessing financial data. The following represent more specific areas where the Board needs to enhance controls over safeguarding computer data.

Computer Data Storage — The internal control system should include policies that require data to be stored on computers that are in an area protected from possible loss due to environmental factors such as climate, fire and water damage. The Board has not established policies or procedures to ensure that both the non-financial data and financial computer system equipment are located in rooms that are climate controlled. The District's information technology (IT) consultant told us that IT staff has had trouble in the summer with the server failing due to excess heat and increased temperature of the equipment. However, during our audit, we found that heat generated by the server equipment was reduced to an acceptable level with the use of fans. Server failures result in additional work for IT staff and a decrease in productivity for employees whose work is interrupted.

Back Up — Data should be backed up (i.e., copy made) on a routine basis and the back up copy stored at an environmentally and physically secure off-site location. We found that the Board has not established policies or procedures for the back up of financial data on the computers. Currently, the financial data is backed up on an external USB hard drive that is attached to the same computer where the data is originally entered and not stored offsite. Therefore, in the event of a disaster causing computer failure also rendering the physical site inaccessible, the back up copy would not be accessible, rendering data unusable or irretrievable. Non-financial data is properly backed up and stored off-site. The District risks losing most, if not all, of their computer-processed financial data and has no means to ensure its recovery in order to continue normal operations.

Disaster Recovery — The internal control system policies should also require the adoption of a formal disaster plan to prevent loss of computer equipment and data and procedures for recovery in the event of a loss. The plan should include precautions to be taken to minimize the effects of a disaster so the organization will be able to either maintain or quickly resume mission-critical functions. The plan may also include a significant focus on disaster prevention.

We found that the Board has not established formal policies or procedures to address potential disasters. In the event of a disaster, District personnel have no guidelines or plan to follow to prevent the loss of equipment and data or data recovery procedures.

Remote Access — Another component of internal controls ensures that remote access (i.e., ability to access the computer from an internet or other external source) is controlled and monitored so that only authorized individuals may enter or retrieve data. Internal controls should include policies and procedures addressing how remote access is granted, who is given remote access and security issues, as well as how remote access will be monitored and controlled.

The Board has not implemented procedures to monitor and control remote access to financial computer data. Currently the IT consultant has full remote access to the financial data, after the District officials open a connection. Additionally, District officials have no procedures in place to provide for an audit trail of the consultant's work within the computer financial system.

Internal controls are greatly weakened when remote access is not monitored or controlled. Financial data could be manipulated and could allow for errors and irregularities to occur and go undetected.

These internal control weaknesses could lead to loss of important financial data along with a serious interruption to District operations, such as not being able to process checks to pay vendors or employees.

Recommendations

1. The Board should adopt policies and procedures to strengthen internal controls relating to computer data storage, backup and disaster recovery.
2. The Board should adopt policies and procedures to control and monitor remote access to financial computer data.

Cash Disbursements

An internal control system, which is established by the Board and implemented by District officials, is the integration of the activities, plans, attitudes, policies and efforts of the District staff to provide reasonable assurance that the District will achieve its objectives. An appropriate system of internal controls over cash disbursements consists of policies and procedures intended to provide reasonable assurance that, among other things, all cash disbursements are for proper District purposes and authorized to be made as well as recorded timely and accurately.

We found that the District's internal controls over cash disbursements were appropriately designed and operating effectively to safeguard cash.

While reviewing the internal controls over cash disbursements, we determined the process in place is as follows: using audited and approved claims as source documents, the Accounts Payable Clerk prepares and prints "check run reports" (listings of checks to be printed) and warrants (listings of audited and approved claims) which she then forwards to the Internal Claims Auditor. The Internal Claims Auditor compares the information on the "check run reports" to the audited claims and signs off on the warrants. The Treasurer then authorizes the payment of the claims and the Accounts Payable Clerk prints the checks, electronically placing the Treasurer's signature on the checks. The Treasurer has custody of the checks until they are mailed by the Accounts Payable Clerk. The Treasurer maintains a monthly listing of checks used to ensure there are no unaccounted for checks and to reconcile all bank accounts. We also found that the blank check paper stocks are pre-numbered and preprinted with District information and are safeguarded by being kept in a locked cabinet, which is accessible by both the Treasurer and Accounts Payable Clerk. As an additional control, the Board reviews the "check run reports."

We examined 200 cash disbursement transactions, about seven percent of all transactions, to determine whether the purchases were properly authorized for payment, the claims were paid for the appropriate amounts and the checks were properly endorsed in accordance with the internal control objectives described above. We found no significant deficiencies in the transactions we examined.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

Tioga Central School

TIOGA CENTER, N. Y. 13845

August 18, 2006

██████████
Office of the State Comptroller
State Office Building Room 1702
44 Hawley Street
Binghamton, NY 13901-4417

Dear ██████████:

Please consider the following items in response to the Report of Examination of the Tioga Central School District for the period July 1, 2004 through June 30, 2006.

Your audit focused on two primary areas: Computer Data Safeguards and Cash Disbursements. We were pleased to note no deficiencies in the cash disbursement area. Your report delineated two recommendations in the computer data area:

- *The Board should adopt policies and procedures to strengthen internal controls relating to computer data storage, backup and disaster recovery.*

The district has conferred with the IT consultant to implement a secondary back-up system. The financial data stored on the administrative server will be backed up on a routine basis and will be stored at an environmentally and physically secure off-site location from the Administration Building. The district will work with the Technology Coordinator and Emergency Management Coordinator to draft a formal disaster plan to prevent loss of computer equipment and data in the event of a catastrophe. This plan will be included in the district's SAVE plan and will be adopted by the Board of Education.

- *The Board should adopt policies and procedures to control and monitor remote access to financial computer data.*

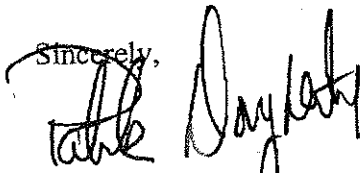
Your report indicated that: "Currently the IT consultant has full remote access to the financial data." We conferred with our IT consultant regarding this finding and do note the following clarification: our IT consultant indicated that he does not have any remote connection to our network without our permission. Our system has a firewall with no

See
Note 1
Page 14

port openings in it to allow access from any source on the outside. In order to access our systems, or network, the IT consultant would use a product called Winx. This product would give him a tracking number which we would allow via the Internet, and then we would have to authorize his access to the network system. This software (Winx) would also provide a log of the access times for an audit trail of any outside entry.

We found the external audit process very helpful. We were pleased to see that overall the district is financially responsible and has effective internal controls. The Board of Education and Administration are committed to ensuring that your recommendations are implemented so that efficient operations and fiscal practices are maintained over time.

Sincerely,



Patrick M. Dougherty
Superintendent of Schools

cc: [REDACTED]

APPENDIX B

OSC COMMENT TO DISTRICT OFFICIALS' RESPONSE

Note 1

We amended our report based upon clarifying information presented to us at our exit conference.

APPENDIX C

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: cash receipts and disbursements, purchasing, payroll and personal services, and capital assets and consumable inventories.

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 objectives and scope by selecting for audit those areas most at risk. We selected safeguarding of computer data and cash disbursements for further audit testing.

In order to accomplish the objectives of this audit, our procedures included the following:

- We reviewed current procedures relating to computer data storage, back up, disaster recovery and remote access controls.
- We reviewed pertinent documents including: cancelled checks, bank statements, warrants, cash disbursement journals and various other accounting records and financial reports to determine if cash disbursement transactions were properly initiated, approved and recorded.
- We compared information included on cancelled checks with related supporting documentation and reviewed it for any unusual, improper or suspicious payees.
- We reviewed bank reconciliations as they pertain to cash disbursements for accuracy, completeness and timeliness.
- We reviewed electronic and/or manually processed cash transfers (which constitute disbursements) for legitimacy, approval and accuracy.

- We viewed the check number sequences used for each fund to ensure that all checks — both used and unused — were properly accounted for.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). Such standards require that we plan and conduct our audit to adequately assess those district operations within our audit scope. Further, those standards require that we understand the district's management controls and those laws, rules and regulations that are relevant to the district's operations included in our scope. An audit includes examining, on a test basis, evidence supporting transactions recorded in accounting and operating records and applying such other auditing procedures, as we consider necessary in the circumstances. We believe that our audit provides a reasonable basis for the findings, conclusions and recommendations contained in this report.

APPENDIX D

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 E
OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT SERVICES
AND ECONOMIC DEVELOPMENT

Mark P. Pattison, Deputy Comptroller
Steven J. Hancox, Assistant Comptroller
John Clarkson, 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

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

Debora Wagner, 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

Christopher J. Ellis, 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, Orange,
Putnam, Rockland, Schenectady, Ulster, Westchester
counties

HAUPPAUGE REGIONAL OFFICE

Richard J. Rennard, 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