Division of Local Government & School A

Table of Contents

found that user accounts were still enabled for 17 individuals who separated from BOCES service anywhere from six months to four years ago. Other users have more access to the system than is required to perform their job duties. Furthermore, although the BOCES' system can generate audit logs, these logs are not reviewed to identify errors or irregularities. As a result, BOCES' IT resource, systems, and its electronic data are subject to increased risk of unauthorized access, manipulation, theft, and loss or destruction of sensitive data.

BOCES officials have adopted a sound credit card policy that clearly outlines when credit cards may be issued and how they are to be used. Furthermore, BOCES officials have developed supplementary

- Have BOCES officials established adequate internal controls over the use of gasoline credit cards, and are those controls operating effectively?

Scope and Methodology

Our overall goal was to assess the adequacy of the internal controls put in place by officials to safeguard BOCES 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 purchasing and information technology areas and, therefore, we examined internal controls over the computerized financial system and gasoline credit cards for the period July 1, 2007 to January 31, 2009. We extended our review of active user accounts to May 2009.

Our audit also disclosed additional areas in need of improvement concerning information technology controls. Because of the sensitivity of this information, certain vulnerabilities are not discussed in this report, but have been communicated to BOCES officials so they could take corrective action.

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 BOCES Officials and Corrective Action

The results of our audit and recommendations have been discussed with BOCES officials and their comments, which appear in Appendix A, have been considered in preparing this report. BOCES 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 GML, Section 2116-a (3)(c) of the Education Law and Section 170.12 of the Regulations of the Commissioner of Education, a written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, with a copy forwarded to the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, R*esponding to an OSC Audit Report*, which you received with the draft audit report. The Board should make the CAP available for public review in the District Clerk's office.

Information Technology

The use of information technology (IT) affects the fundamental manner in which BOCES initiates, processes, records, and reports transactions. The extent to which computer processing is used in significant accounting applications, and the complexity of that processing, determines the specific risks that IT poses to the BOCES' internal controls. The widespread use of IT by BOCES presents a number of internal control risks that must be addressed, including unauthorized access to data, unauthorized changes to data in master files, and the potential loss of data. An effective system of internal controls to safeguard computerized data includes policies and procedures adopted by the Board to minimize the loss or corruption of essential data. It is also important that audit logs are generated and reviewed on a regular basis to detect errors and irregularities.

The IT Director is responsible for the overall day-to-day operations of the BOCES' computer systems. BOCES uses a financial software program (financial software) developed by BOCES staff to process and maintain financial transactions. This financial software consists of modules that segregate various financial recording and reporting processes. Access privileges within the financial software include the ability to add, update, delete, and print transactions within these modules. The financial software is also capable of generating an audit log. At the time of our audit, 276 users had access to the financial software.

BOCES officials have not adopted comprehensive IT policies and procedures that provide guidance to BOCES employees on all aspects and appropriate use of IT systems and data. Additionally, BOCES did not effectively safeguard its computer data. We found that user accounts were still enabled for 17 individuals who separated from BOCES service anywhere from six months to four years ago. Other users have more access to the system than is required to perform their job duties. Furthermore, although the BOCES' system can generate audit logs, these logs are not reviewed to identify errors or irregularities. As a result, BOCES' IT resources, systems, and its electronic data are subject to increased risk of unauthorized access, manipulation, theft, and loss or destruction of sensitive data.

Policies and Procedures

Policies and procedures addressing IT operations are an integral part of an internal control system. BOCES officials are responsible for establishing policies and procedures that provide guidance to employees on all aspects of IT. It is important that these policies include, at a minimum, acceptable-use standards for computer

include detailed guidelines for the proper use of IT resources and the review of audit logs.

2. BOCES officials should review and revise user access rights to the financial software along with job descriptions to ensure that users have access only to transactions within the scope of their responsibilities.

3. BOCES officials should ensure that access is revoked and user accounts deactivated immediately upon an employee's separation from BOCES employment.

4. BOCES officials should ensure that an individual outside of the business process periodically reviews the audit logs generated by the financial software and reports the results of the review.

Gasoline Credit Cards

An effective system of internal controls over the use of BOCES credit cards requires the Board to establish a sound credit card policy, which establishes the parameters for credit card use and the procedures for monitoring credit card use. In order to adequately protect BOCES assets, it is important that the policy require that all credit cards remain in the custody of BOCES officials.

BOCES has issued 25 gasoline credit cards through four separate vendors. Ten of these cards are held in the Business Office as "extras," available for employees to sign out on a temporary basis to use for gasoline expenditures incurred during authorized job-related travel; two cards are assigned for use to the Maintenance & Operations department, and the remaining 13 cards are assigned to eight BOCES administrators and staff (one of the eight administrators is assigned two gas cards, and another two administrators are each assigned three gas cards). During our audit period, BOCES' gasoline expenditures totaled $72,274.

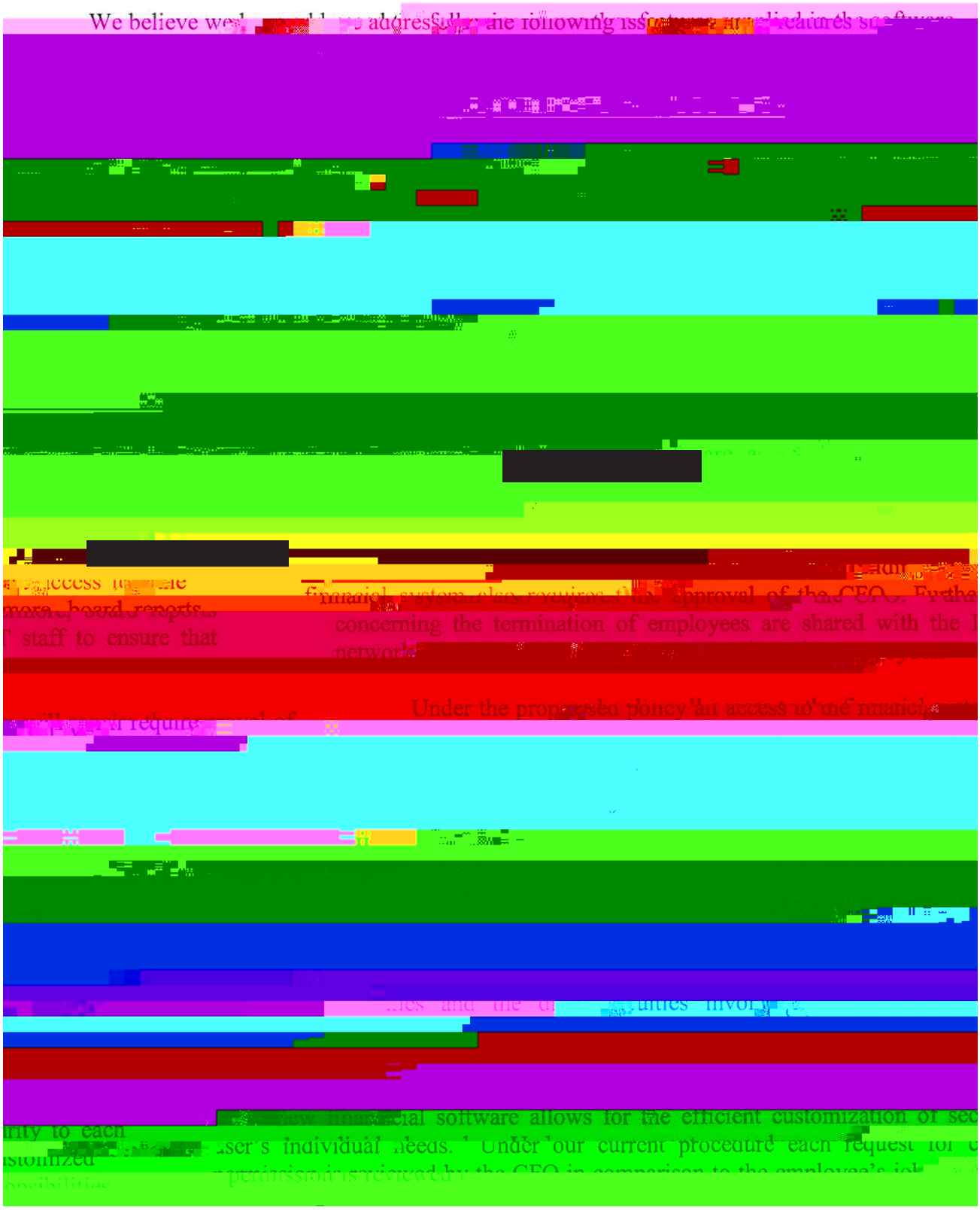
BOCES officials have adopted a sound credit card policy that clearly outlines when credit cards may be issued and how they are to be used. Furthermore, BOCES officials have developed supplementary procedures which require that all purchases of gasoline for BOCES vehicles must be recorded in a log maintained in each vehicle, and any staff holding a BOCES gasoline credit card must submit all of their receipts to the Business Office.

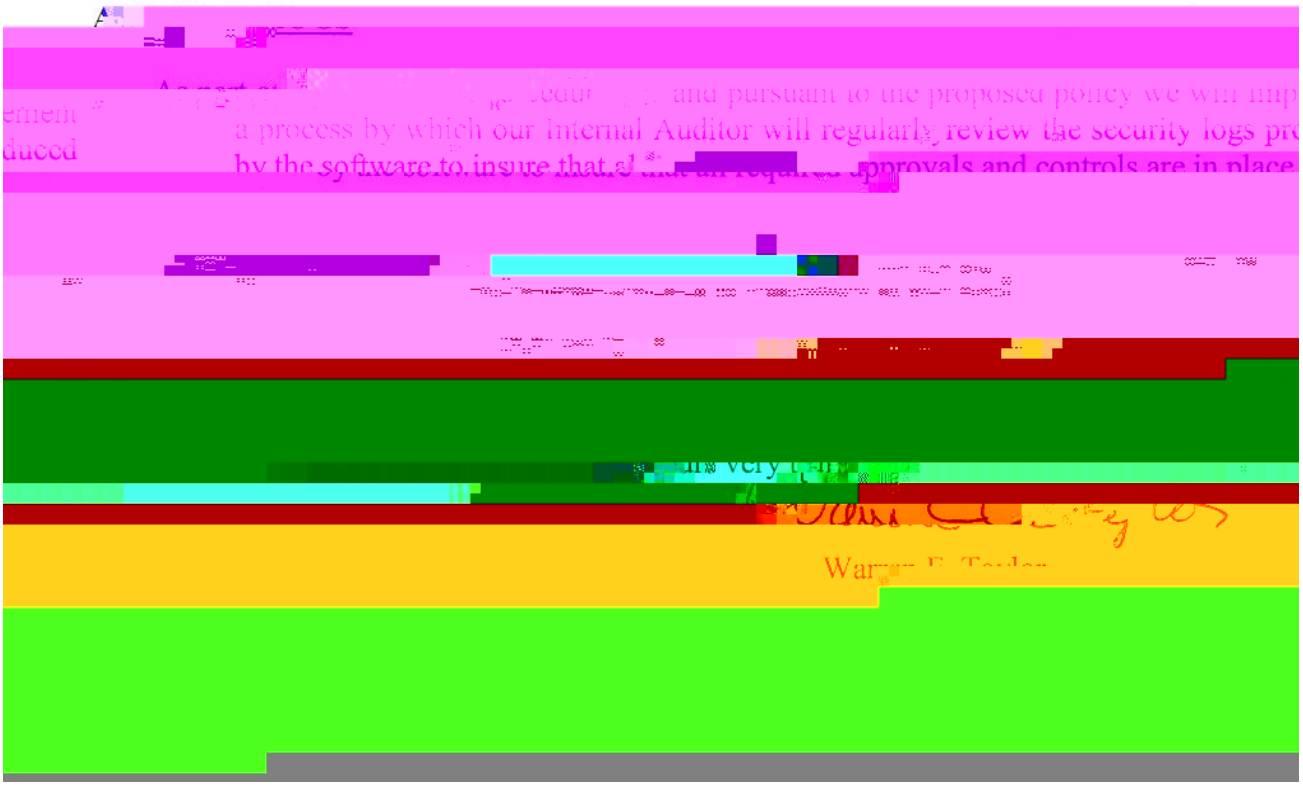
We examined 359 gasoline purchases, totaling $27,466, made from May 1, 2008 through October 7, 2008. Our testing revealed only minor discrepancies in the BOCES' adherence to these policies, which we discussed with BOCES officials to help them improve controls in this area.

APPENDIX A

RESPONSE FROM BOCES OFFICIALS

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





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 BOCES 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 BOCES officials, performed limited tests of transactions and reviewed pertinent documents, such as BOCES 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 BOCES' financial transactions as recorded in its databases. Further, we reviewed the BOCES' 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 gasoline credit cards and the IT system for further audit testing.

During this audit, we examined records and reports of the BOCES for the period of July 1, 2007 to January 31, 2009. To accomplish the objective of the audit and obtain valid evidence, our procedures included the following:

- We interviewed appropriate BOCES officials in order to obtain an understanding of the organization, the BOCES' accounting system, and to identify key personnel.

- We obtained copies of BOCES policies, administrative regulations, and procedures and evaluated the adequacy of these policies.

- We interviewed BOCES staff to obtain an understanding of procedures in place to ensure compliance with the Board-adopted policies.

- We reviewed the minutes of the proceedings of the Board.

- We interviewed the Director of IT and physically inspected the BOCES' IT equipment.

- We reviewed user permissions reports for the financial software and verified the user access controls in the system.

- We interviewed BOCES officials to determine employees' roles and responsibilities and whether they agreed to the permissions reports.

- We reviewed gasoline credit card activity and reconciled a sample of credit card invoices to the logs maintained in each BOCES vehicle.

- We analyzed the gallons purchased and the miles per gallon achieved by each vehicle to determine whether the frequency and size of gasoline purchases appeared to be reasonable.

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

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

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

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