Orange County Community College
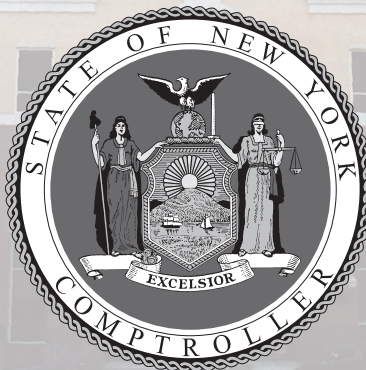
Information Technology and Financial Activities

Report of Examination

Period Covered:

September 1, 2015 — December 1, 2016

2017M-111

Thomas P. DiNapoli

Table of Contents

Page

State of New York
Office of the State Comptroller

**Division of Local Government
and School Accountability**

September 2017

Dear Community College Officials:

A top priority of the Office of the State Comptroller is to help college officials manage government resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support college operations. The Comptroller oversees the fiscal affairs of colleges statewide, as well as 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 college operations and Board of Trustee governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard college assets.

Following is a report of our audit of the Orange County Community College, entitled Information Technology and Financial Activities. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law.

This audit's results and recommendations are resources for college 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*

Orange County Community College (College) is governed by a Board of Trustees (Board) composed of nine appointed members and one elected student trustee.   The Board is responsible for establishing and monitoring the general management and control of College financial and educational affairs. The President of the College (President) is the chief executive officer. The Vice President of Administration and Finance (Vice President) serves as the chief financial officer. The President and Vice President, along with other administrative staff, are responsible for the College's day-to-day management under the Board's direction.

The information technology (IT) department is headed by the chief information officer (CIO) who is responsible for overseeing the College's IT operations and functions, including supervising IT department staff. The College's Director of Student Accounts (Director) is responsible for managing the student accounts office (office) and reports directly to the Comptroller. In addition to receiving College tuition and other fee payments, office staff is responsible for billing students, collecting tuition and other student-related fee payments, issuing refund checks and enforcing delinquent student accounts.

The College has an enrollment of approximately 5,500 students. The College's expenditures for 2015-16 were approximately $85 million, which were funded primarily with County aid, student tuition and related fees, State aid and grants.

The College has experienced turnover in administration within the last several years mostly due to retirement. For example, the current College President has been in office since June 2015. Similarly, the Vice President, the Comptroller, the Director of Payroll, the Interim CIO and the Purchasing Coordinator have been in office for less than three years.

Scope and Objectives

The objectives of our audit were to examine the College's controls over IT and financial activities for the period September 1, 2015 through December 1, 2016. We extended our audit scope through March 15, 2017 to review student account balances. Our audit addressed the following related questions:

Did College officials:

- Ensure that the IT systems were adequately secured and protected against unauthorized use, access and loss?

- Procure goods and services in accordance with applicable statutes?

- Ensure that claims were properly authorized, supported and for legitimate College purposes?

- Ensure student accounts are properly billed, collected, enforced and that adjustments and refunds were properly approved and applied?

Audit Results

College officials need to improve IT controls to help ensure that data is adequately secured and protected against unauthorized use. The Board did not adopt adequate IT policies that address appropriate computer use and security or provide training on its policies, cybersecurity and financial software application. We also found that employees had excessive rights to computer software.

The lack of adequate controls has led to unauthorized personal Internet use. The servers and server rooms were not adequately protected, backups were not adequately maintained and a disaster recovery plan has not been established to safeguard IT assets from internal and external threats. Furthermore, computer equipment inventories are not being properly maintained to help control IT assets. As a result, there is an increased risk that IT assets (data, hardware and software systems) may be lost or damaged by inappropriate access and use.

The Board also needs to improve its purchasing procedures to ensure College officials procure goods and services in accordance with applicable statutes. The Board purchasing policy is inadequate because it does not address all General Municipal Law (GML) requirements and College officials did not comply with these requirements when procuring goods and services. In addition, the Board did not identify a purchasing agent independent from the cash disbursement process to approve purchases.

Also, although the Board awarded the $101,840 in purchase contracts using what they believed was a "best value" method, the awards did not adhere to the GML best value method requirements. As a result, the College may have incurred higher costs than necessary or, in the case of best value, may not have optimized quality, cost and efficiency for the items it acquired. Further, the Board does not have adequate assurance that purchases were made without favoritism, improvidence or extravagance and goods and services may not have been acquired in the residents' best interest.

College officials did not ensure that claims were properly authorized, supported and for legitimate College purposes. Officials did not have any written procedures documenting the claims process. In addition, the President did not appoint an official claims auditor. The Comptroller and Assistant Comptroller (Assistant) are responsible for auditing claims. However, the Comptroller is responsible for authorizing purchases and the Assistant is involved in the disbursement process, duties which are incompatible with auditing claims. Further, reports were not prepared and issued to the President after the claims audits were complete to document the audit results.

Our review of 75 claims totaling almost $104,500 and 220 credit card charges totaling approximately $20,900 disclosed that department heads did not approve purchase requisitions and the Comptroller did not authorize claims before goods were received. Claims did not contain documentation showing goods were received, were paid without an original itemized invoice and rates paid did not agree with contract agreements. Also, sales tax was charged on credit cards and College officials were unable to

determine whether nine credit card charges totaling $623 were for proper College purposes because no documentation supporting these charges was maintained.

Finally, College officials need to improve controls in the student accounts office (office) to ensure student accounts are properly enforced if delinquent, and adjustments are properly approved and applied. Policies and procedures over student accounts were insufficient and not approved by the Board. Office staff made undocumented and unsupported adjustments to student accounts with minimal oversight. Duties within the office were not adequately segregated and College officials did not implement compensating controls, such as providing additional reviews and approvals. As a result, there is an increased risk that errors or unauthorized adjustments could be made that are undetected and uncorrected.

Generally, students were accurately billed, tuition was accurately collected and refunds were appropriately applied. However, account adjustments were made without appropriate approval and delinquent accounts were not always adequately enforced. We tested 15 student accounts with promissory notes totaling $23,155 and determined that three accounts had inaccurate amounts paid, five accounts were past due and payment on six accounts were not received in consecutive monthly installments as specified by the promissory notes. When promissory note payments are not current, the College is not receiving funds as agreed upon.

Comments of College Officials

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

Introduction

Background

Orange County Community College (College) is located in Orange County, has two campuses and about 5,500 students. The College is governed by a Board of Trustees (Board) composed of nine appointed members and one elected student trustee. The Board is responsible for establishing and monitoring the general management and control of College financial and educational affairs. The President of the College (President) is the chief executive officer. The Vice President of Administration and Finance (Vice President) serves as the chief financial officer. The President and Vice President, along with other administrative staff, are responsible for the College's day-to-day management under the Board's direction. Expenditures for 2015-16 were approximately $85 million, which were funded primarily with County aid, student tuition and fees, State aid and various grants.

The information technology (IT) department is headed by the chief information officer (CIO) who is responsible for overseeing the College's IT operations and functions, including supervising IT department staff and securing approximately 2,700 computers. The Director of Student Accounts (Director) is responsible for managing the student account office (office) and reports directly to the Comptroller. In addition to collecting College tuition and other fee payments, office staff is responsible for billing students, issuing refund checks, issuing student account adjustments and enforcing delinquent student accounts.

The College has experienced turnover in administration within the last several years mostly due to retirement. For example, the current College President has been in office since June 2015. Similarly, the Vice President, the Comptroller, the Director of Payroll, the Interim CIO and the Purchasing Coordinator have been in office for less than three years.

Objectives

The objectives of our audit were to examine the College's controls over IT and financial activities for the period September 1, 2015 through December 1, 2016. Our audit addressed the following related questions:

Did College officials:

- Ensure that the IT systems were adequately secured and protected against unauthorized use, access and loss?

- Procure goods and services in accordance with applicable statutes?

- Ensure that claims were properly authorized, supported and for legitimate purposes?

- Ensure student accounts were properly billed, collected, enforced and that adjustments and refunds were properly approved and applied?

Scope and Methodology

We examined the College's controls over IT and financial activities for the period September 1, 2015 through December 1, 2016. We extended our audit scope through March 15, 2017 to review student account balances. Our audit also examined the adequacy of certain IT controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to College officials.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix B of this report. Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or relevant population size and the sample selected for examination.

Comments of College Officials and Corrective Action

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

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and forwarded to our office within 90 days, pursuant to Section 35 of General Municipal Law. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. We encourage the Board to make this plan available for public review in the President's office.

Information Technology

The College uses IT systems for computer education, Internet access, email communications, student data storage and to maintain financial records. The use of IT affects the fundamental manner in which transactions are initiated, recorded, processed and reported. If the computers on which IT data is stored fail or the data is lost or altered, the results could range from inconvenient to catastrophic. Even small disruptions can require extensive effort to evaluate and repair. College officials are responsible for designing and implementing internal controls over IT systems. IT controls help to ensure that computer systems and the data they process, transmit and store can be trusted, are available when needed, and are adequately protected from unauthorized access and use.

College officials need to improve IT controls to help ensure that data is adequately secured and protected against unauthorized use. The Board did not adopt IT policies that address appropriate computer use and security or provide training on computer policies, cybersecurity and financial software application. College staff have excessive access rights to the network, financial application and online banking that are not needed for their job functions. As a result, there is an increased risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

We identified unauthorized personal Internet use during work hours, which increases the risk of employee time abuse, lost resources and exposes the network to significant threats. The IT servers and infrastructure did not have adequate protection, backups were not adequately maintained and a disaster recovery plan was not implemented to safeguard IT assets from internal and external threats. Furthermore, computer equipment inventories were not properly maintained to help control IT assets.

Computer Policies and Training

Computer policies define appropriate user behavior, describe the tools and procedures needed to protect data and information systems and explain the consequences of policy violations. To provide important oversight and leadership, the Board should establish computer policies that take into account people, processes and technology, communicate the policies throughout the organization and ensure there are procedures in place to monitor compliance with policies.

Breach Notification Policy – An individual's private or financial information, along with confidential business information, could be severely affected if security is breached or personal data is

improperly disclosed. New York State Technology Law requires a breach notification policy be adopted to detail how College officials would notify individuals whose private information was, or is reasonably believed to have been, acquired by a person without a valid authorization. The disclosure should be made in the most expedient time possible, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and reasonably restore data system integrity.

The Board has not adopted a breach notification policy. As a result, in the event that private information is compromised, College officials and employees may not understand their responsibilities or be prepared to notify affected individuals.

Internet, Email and Personal Computer Use Policy – This policy should describe what constitutes appropriate and inappropriate use of IT resources, along with expectations concerning personal use of IT equipment and user privacy. It should also describe the consequences for policy violations.

The College's computer use policy is inadequate because it does not describe what constitutes appropriate and inappropriate use of IT resources, the expectations concerning personal use of IT equipment, user privacy and consequences for policy violations. In addition, College officials do not require users to sign an acceptable use policy acknowledgement and monitor or enforce computer use.

College officials were unaware that the internet, email, and personal computer use policy was inadequate. These inadequate policies result in an increased risk that data, hardware and software systems may be lost or damaged by inappropriate access and use.

Personal, Private and Sensitive Information (PPSI) Policy – This policy should define PPSI, explain the College's reasons for collecting PPSI and describe specific procedures for the use, access to, storage and disposal of PPSI involved in normal business activities. The College does not have a policy addressing PPSI. As a result, there is a significant risk that individuals may access PPSI without a valid authorization and sensitive information may become compromised.

Password Security Policy – This policy should address password complexity, length, age requirements, reuse of old passwords and the number of failed log-on attempts the system will allow. The Board has not adopted a password security policy. As a result, there is a significant risk that data, hardware and software systems may be damaged or stolen by inappropriate access and use.

Wireless Security Policy – This policy should specify the conditions that wireless devices must satisfy to connect to the College's network. The policy should also indicate who is covered by the policy and describe the consequences of violating the policy. The Board did not adopt a wireless security policy. College officials were unaware that it was needed. Without this policy, there is an increased risk that the College's wireless network may be inappropriately accessed and the data and software systems may be used inappropriately or damaged.

Mobile Computing and Storage Device Policy – The purpose of this policy is to control mobile computing and storage devices that contain or access College information resources. It should define the devices covered, procedures for reporting lost or stolen devices, the process used for gaining approval before connecting new devices to the system and other user responsibilities. The Board has not adopted a mobile computing and storage device policy. As a result, there is increase risk that hardware and data may be lost, damaged or stolen.

Online Banking Policy – This policy should address what online banking activities will be used, what specific transaction types will be allowed, who will authorize transactions and record transactions or transfers, who has access to online banking, who will review and reconcile transfers, and how often, and the procedures that will be followed when responding to inappropriate activity.

The College uses online banking, but the Board has not adopted an online banking policy. This increases the risk that college revenues could be inappropriately disbursed.

IT Equipment Inventory Policy – This policy should outline guidance and procedures for establishing and maintaining controls over IT equipment and should include the major types of equipment, identify employees responsible for physically safeguarding these assets, a description specifying the types of inventory records that should be maintained and the employees responsible for maintaining these records.

The Board has not adopted an IT equipment inventory policy. Without a policy there is an increased risk that hardware and software systems may be lost, damaged or stolen.

IT Security Training and Awareness – A well-informed work force is the strongest link in the chain to secure electronic data and computer systems. Organizations cannot protect the confidentiality, integrity and availability of their data and systems without ensuring that the employees using and managing IT understand IT security policies and procedures and their roles and responsibilities.

College officials did not provide training on cybersecurity and provided limited training on the College's financial software application. Officials told us that training has not been provided because of limited IT personnel staffing. If officials do not provide sufficient training on existing IT policies, cybersecurity awareness and the financial software, there is an increased risk that users will not understand their responsibilities, which puts the data and computer resources with which they have been entrusted at greater risk for unauthorized access, misuse or abuse.

Access Rights

Computer access controls specify the employees and computer processes that have access to a specific computer resource, such as a particular software program or database. Access rights should be updated as necessary and generic user accounts and dormant accounts should be disabled or removed from the network in a timely manner. In addition, IT administrators should monitor user access into the network and control and monitor remote access by limiting access through ports and reviewing firewall or software audit logs. Employee access rights should be limited to those specific functions necessary to perform their individual job duties.

College officials have not established written procedures for use of the financial software application. In addition, officials have not implemented standard processes for granting, revoking or modifying individual network access rights. Currently when an employee is hired, the Assistant sends an email to IT staff with the employee name and title but the email does not specify the access rights that should be granted based on job duties. Officials have not set a standard period of time after which user accounts for those employees leaving College employment are to be removed. Also, College officials do not maintain and periodically review authorized users and their network or financial software access levels.

We evaluated financial software access granted to 15 employees and found that all of them had excessive user rights based on their job duties. In addition, we reviewed online banking rights for 10 employees and found 9 of them had excessive user rights based on job duties. College IT administrators did not monitor user access to the network and although remote access was recorded, such access was not reviewed. As a result, there is increased risk that users could inappropriately access data and programs. Furthermore, IT administrators would be unable to detect whether users are accessing unauthorized applications or high risk data.

Personal Internet Use

While using the Internet is a nearly indispensable resource for conducting business, users are susceptible to significant threats from cybercriminals who exploit the vulnerabilities of IT systems to gain

unauthorized access to sensitive data. Internet browsing increases the likelihood that users will be exposed to malware[1] that may compromise data confidentiality. College officials can reduce the risks to sensitive data and IT assets by monitoring Internet use and using web filtering software to block access to unacceptable websites.

We selected and reviewed Internet browsing histories of 15 computers[2] to determine whether there were any instances of unauthorized Internet use. Browsing histories for 12 of these computers showed instances of unauthorized personal Internet use. The types of websites found included social networking, personal email, online dating, entertainment and personal banking, shopping and travel sites visited while using the College's computers during normal work hours. Additionally, several computers had downloaded adware that was not detected or removed.

Inappropriate use occurred because the computer use policy was inadequate and IT administrators did not review user logs, monitor Internet use or configure the web filtering software to block access to these sites. Inappropriate use of College computers could potentially expose the network to virus attacks or compromise systems and data, including key financial and confidential information. Furthermore, time spent by employees during work hours using College resources for personal reasons represents lost resources and potential time abuse.

Server Room Security

Physical security controls restrict access to computer resources and help protect these resources from intentional or unintentional harm, loss or impairment. Controls include guards, gates, locks and environmental controls such as smoke detectors, fire alarms and extinguishers, water damage protection and uninterruptible power supplies.

The College has three server rooms only one of which has a fire suppression system. Although two server rooms have fire extinguishers and smoke detectors, neither of these rooms have fire suppression systems. In addition, even though each server has a battery back-up that will last 20 minutes, servers are not connected to a dedicated generator in case of a sustained power outage. Instead, the servers are linked to a generator that will turn on, if the entire College campus loses power. Further, there are no keypad or entrance logs for two server rooms. Finally, one server room has manual heating and air

---

[1] Malware infiltrates a computer system by circumventing network defenses, avoiding detection and resisting efforts to disable it.

[2] We reviewed 10 business office computers and five student account department computers. Two computers did not have any Internet browsing histories.

conditioning units with temperature controls, but no central cooling system.

College officials told us that they have slowly been updating the outdated IT environment. However, officials have been hampered in their efforts to complete all necessary upgrades due to a high rate of turnover in key IT personnel and limited financial resources. As a result of these poor physical security controls and absence of a long-term source of reliable power, there is an increased risk that IT assets could be compromised by internal, external or environmental factors resulting in an interruption of service.

Backups

A backup is a copy of electronic information that is maintained for use if there is loss or damage to the original. Backup procedures are a necessary part of IT contingency planning and are critical for restoring operations quickly and effectively following a service disruption.

College officials have not adopted written procedures specifying how systems should be backed up or backup frequency. The College uses a site-to-site backup between campuses and one backup or daily file copy is maintained. However, in the event of data corruption that is not discovered that day, the uncorrupted data will be written over and cannot be retrieved. In addition, backups of sensitive data are not encrypted and backups are not tested to ensure the data is available or the backup process is running correctly. College officials are unaware when the last backup was tested. Officials told us that these deficiencies occurred due to the high turnover of key IT personnel and the system's inability to create multiple backups.

By not establishing written procedures on how systems are backed up, officials may not be able to recover backup data and crucial data may not be backed up. By not maintaining multiple backups, there is a higher risk that data from a previous backup, containing information that may be necessary to restore, will be overwritten during the next backup. In addition, not encrypting backup data leaves the data vulnerable to unauthorized users. By not periodically restoring backups for testing purposes, IT administrators do not have adequate assurance that they can restore data after an emergency.

Disaster Recovery Plan

The Board is responsible for adopting a comprehensive IT security plan that includes a disaster recovery plan to prevent or minimize the loss of computerized equipment and data and provide procedures for recovery in the event of an actual loss. A disaster recovery plan provides guidance for how employees should communicate, where they will go and how they will perform their jobs in the event of a disaster. The plan could include an alternate processing location and plan to procure computers with appropriate software to resume

normal operations as soon as possible. It may also include the types of threats to the IT system, an analysis of business processes, continuity needs, the roles of key individuals and a focus on disaster prevention. The disaster recovery plan should be periodically tested to ensure it works as intended and that users know their duties should a disaster occur.

The Board has not adopted a disaster recovery plan and employees have not been notified or trained on the procedures to follow in case of a disaster. As a result, if an emergency occurs, employees do not have guidance for restoring data or resuming critical operations in a timely manner. In addition, employees may not know their emergency job functions and operations may not be resumed as quickly as possible. The lack of an adequate disaster recovery plan could lead to loss of important financial and confidential data and interruption of the College's operations.

Computer Equipment Inventory

Computer equipment inventory records should contain descriptions, quantities, locations, dates of purchase and original cost and, when appropriate, assign responsibility for the asset to a specific official or manager. Detailed records make verifying the existence of computer equipment easier and demonstrates to employees that management is monitoring purchases and use, deterring theft and misuse. Assigning responsibility to a specific employee holds that person accountable for safeguarding computer equipment.

We reviewed inventory records for 10 computers and found that cost information was not included. Additionally, seven computers had inaccurate locations listed. College officials were only able to provide each computer's location after a detailed search. We tested the inventory records for another 15 computers and found that five computers were not listed on the inventory records.

College officials told us that equipment inventory records are not properly maintained due to the high turnover of key IT personnel and limited staff. Without a current and complete computer equipment inventory, the risk of loss or misuse is increased because the College officials are unable to properly monitor equipment purchases and use.

Recommendations

The Board should:

1. Establish and adopt a breach notification policy.

2. Review and update the existing Internet, email and personal computer use policy to include a description of appropriate and inappropriate use of IT resources and expectations concerning the personal use of IT equipment and user privacy.

3. Establish and adopt IT policies relating to PPSI, password security, wireless security, mobile computing and storage device, online banking and equipment inventory.

4. Adopt a formal written disaster recovery plan.

The CIO should:

5. Require all users to sign an acknowledgment form indicating they have read the IT policies (including a computer use policy) and monitor and enforce computer use.

6. Provide adequate training relating to cybersecurity, IT policies and the financial software application.

7. Establish written procedures for granting, changing and revoking user access rights to the network and software applications.

8. Establish a standard period of time after which user accounts for those employees leaving College employment are to be removed. Deactivate those user accounts with access to all computer-related applications after the set time period.

9. Maintain and review a current list of authorized users and their network access levels and establish a reasonable period of time to terminate dormant accounts.

10. Control and monitor remote user access to the network.

11. Maintain and periodically review a list of authorized users and their access levels to the financial software and restrict user access rights to those that employees need to perform their job duties.

12. Establish written procedures for the use of the financial application and ensure there are processes in place to identify any training needs.

13. Establish guidelines for authorized Internet use and monitor computers for any unauthorized use.

14. Improve server rooms' physical security by installing fire suppression systems, automatic temperature controls, a designated generator and entry keypads or logs.

15. Establish a method of maintaining multiple backups without overwriting previous data each time a new back up is created.

16. Establish written procedures describing the frequency, location and scope of backups and the specific methods used to backup data.

17. Encrypt all sensitive backup data.

18. Periodically restore backups to ensure the restoration process works as intended.

19. Develop a disaster recovery plan and test it periodically to ensure it works as intended.

20. Review and update all computer equipment inventory records to ensure they are complete and contain accurate descriptions, quantities, locations, date of purchase and original cost.

College officials should:

21. Immediately notify IT administration in writing when an individual leaves College employment and retain the notification.

The Vice President of Administration should:

22. Ensure the proper segregation of duties and regularly review permission rights for online banking to ensure an employee does not have more rights than what is necessary for their job duties.

General Municipal Law (GML) generally requires the Board to advertise for bids on contracts for public works involving expenditures of more than $35,000 and on purchase contracts involving expenditures of more than $20,000. Purchase contracts that exceed the statutory threshold may be awarded on the basis of best value[3] as an alternative to an award to the lowest responsible bidder.

GML further stipulates that the Board must procure goods and services, which are not required by law to be procured by competitive bid, in a manner to assure the prudent and economical use of public money. Procurement of goods and services should be of maximum quality at the lowest possible cost under the circumstances and should guard against favoritism, improvidence, extravagance, fraud and abuse.

The Board needs to improve its purchasing procedures to ensure College officials procure goods and services in accordance with applicable statutes. College officials did not ensure that competitive procurement procedures were always followed to obtain goods and services at the lowest possible price. The Board's purchasing policy is inadequate because it does not address all GML requirements and College officials did not comply with those requirements when procuring goods and services. In addition, the Board did not identify a purchasing agent independent from the cash disbursement process to approve purchases. Although the Board awarded $101,840 in purchase contracts using what they believed was a best value method, the awards did not adhere to GML best value method requirements.

As a result, the College may have incurred higher costs than necessary or, in the case of best value, may not have optimized quality, cost and efficiency for the items it acquired. Further, the Board does not have adequate assurance that purchases were made without favoritism, improvidence or extravagance and goods and services may not have been acquired in the residents' best interest.

Policies and Procedures

GML requires the Board to adopt written policies and procedures governing the procurement of goods and services that are not subject to competitive bidding requirements, such as items that fall below the dollar thresholds and professional services. These policies and procedures should indicate when College officials must obtain

---

[3] For this purpose, best value is defined, in part, as a basis for awarding contracts to the offeror that optimize quality, cost and efficiency among responsive and responsible offerors. In assessing best value, non-price factors may be considered when awarding the purchase contract. See GML Section 103.

competition, outline the procedures for determining the competitive method that will be used and provide for adequate documentation of the actions taken.

The Board's purchasing policy was insufficient because it did not include GML requirements for competitive bidding or contain guidelines or purchasing thresholds for procuring goods and services including professional services, which are not required to be competitively bid. Additionally, College officials did not establish written policies relating to purchasing procedures or the employees responsible for the purchasing process and were unaware of these policy deficiencies. As a result, there is a risk that officials will not comply with GML when making purchases or obtain goods and services of maximum quality at the lowest possible cost.

Purchasing Agent

The Board should identify a purchasing agent or designate someone independent from the cash disbursement process to approve College purchases. Segregating incompatible duties is an internal control practice that can reduce the risk that employees are able to initiate inappropriate transactions without being detected. The objective of segregating duties is to prevent one employee from having access to assets and responsibility for maintaining the accountability or authorizing transactions affecting those assets. When it is neither practical nor cost-effective to segregate basic responsibilities, compensating controls, such as additional supervisory review, should be implemented.

The College Comptroller (Comptroller) reviews purchase requisitions and approves all credit card charges and purchase orders for items costing more than $1,000 (the principal purchasing clerk authorizes all other purchases). In addition, the Comptroller is an authorized signatory on the bank account, authorizes claims for payment and signs the checks. Because the Comptroller's duties allow her to create and execute purchase orders, approve them and sign checks, there is an increased risk that inappropriate transactions could be processed. College officials were unaware that GML allows the Board to designate an agent to approve purchases and did not consider the risk of allowing the Comptroller to have incompatible duties without implementing compensating controls.

Competitive Procurement

While College officials may award a purchase contract on the basis of best value rather than lowest responsible bidder, specifications for a best value award should describe the general manner in which the evaluation and award will be conducted and identify the relative importance of weighing price and non-price factors. When the College awards a purchase contract on the basis of best value, it must

be based on objective and quantifiable analysis, such as a cost-benefit, whenever possible.

The Board must adopt policies and procedures that indicate when College officials need to seek competition for professional services through methods such as issuing requests for proposals (RFP). An RFP is a structured document that specifies minimally acceptable functional, technical and contractual requirements, and the evaluation criteria that will govern the contract award.

While College officials are not legally required to seek competition when soliciting professional services, doing so helps ensure that the College obtains needed services at a reasonable price, from qualified professionals, in the residents' best interests without partiality.

The Board's purchasing policy required three written quotes for the procurement of materials, supplies and some services costing more than $1,000 but less than $20,000 and in accordance with GML a sealed public bid is required for contracts of more than $20,000. However, the purchasing policy did not include policies and procedures for procuring professional services. Therefore, College personnel do not have any written guidance to follow regarding soliciting professional service providers.

The College paid 69 vendors approximately $3.3 million during the audit period for purchases for which College officials should have solicited competitive bids or obtained quotes. We reviewed payments made to 25 vendors who received an aggregate total of approximately $2 million for which officials were required to obtain competitive bids or quotes.

Purchases from 10 vendors, paid approximately $534,000, were not competitively bid as required. For example, one vendor supplied water treatment services totaling $101,840 that were not bid. However, quotes were obtained but the job was not awarded to the vendor with the lowest quote and no documentation was maintained supporting these purchases as best value. In addition, two of the 10 vendors were paid $147,316 for software and $63,781 for smoke detectors without bids or competitive quotes.

We also reviewed payments to 20 professional service providers paid an aggregate of approximately $2.5 million of the 34 service providers paid approximately $3.3 million during our audit period. There was no evidence on file indicating that the College sought competition for 12 of these providers paid $788,059. These purchases were for services such as advertising, accounting, inspection, billing, training, CIO staff and sign language. In addition, four service providers were

collection agencies paid fees totaling $234,756 without sufficient documentation supporting the cases assigned. Further, collection cases were not assigned to the agency with the lowest rate but to all four agencies based on other factors such as experience.

Because the purchasing process was decentralized (not all purchase orders were handled through the purchasing department) and sufficient documentation was not maintained, there is an increased risk that the College did not obtain goods or services of the best quality at the lowest possible cost.

Recommendations

The Board should:

23. Amend its purchasing policy and written procedures to comply with GML.

24. Ensure College officials use competitive procedures when procuring goods and ensure that competitive bids or competitive offers are awarded in accordance with GML.

25. Identify or designate an individual or purchasing agent independent of the cash disbursement process to approve all purchases.

The Vice President should:

26. Ensure that the individual designated to approve purchases reviews them for compliance with GML and College policy before approving purchases.

Claims

The Board is responsible for the audit of claims, but may delegate this responsibility to a claims auditor. To ensure duties are properly segregated, the claims auditor should be independent of the purchasing and disbursement functions. An effective claims auditing system ensures that tax dollars are spent efficiently by requiring a thorough, deliberate and independent audit of claims before payments are authorized. In addition, the Board should adopt a credit card policy to address the specific circumstances under which credit cards may be used.

The Board did not ensure that claims were properly authorized, supported and for legitimate College purposes. Officials did not have any written procedures documenting the claims process and for processing credit card payments and the Board did not adopt a credit card policy. In addition, the Board did not appoint an official claims auditor and reports were not generated after a claims audit was completed.

Our review of 75 claims totaling almost $104,500 and 220 credit card charges totaling approximately $20,900 disclosed several deficiencies. For example, department heads did not approve purchase requisitions, contracts or rates were not attached to the vouchers and claims were not authorized by the Comptroller before goods were received or contain any documentation showing that the goods were received. Further, claims were paid without original itemized invoices and the rates paid did not agree with the purchase contracts.

In addition, sales tax was charged on credit cards and College officials were unable to determine whether nine credit card charges totaling $623 were for proper purposes because no documentation supporting these charges was maintained. As a result, officials do not have adequate assurance that claims paid are for valid and appropriate College expenditures.

Claims Auditor and Credit Card Policy

When the Board delegates its authority to a claims auditor, the claims auditor should be provided with a job description and other guidance to communicate the auditor's responsibilities. The claims auditor should indicate approval of claims by signing or initialing each individual voucher packet or an abstract of audited claims. Additionally, the claims auditor should report the claims auditing results to the President and suitable records should be maintained to identify the claims audited and whether they were allowed or disallowed, in whole or in part.

The Board should adopt a credit card policy to address the specific circumstances under which credit cards may be used, including those employees authorized to use them, prior approvals needed, dollar limits, the types of expenditures for which they may be used and the documentation that must be presented to support the claim submitted for audit. The policy should also include procedures to monitor credit card use to assess the nature and number of charges for reasonability and promote accountability and responsibility by outlining the associated risks, such as liability for damage, loss or improper use.

College officials did not establish written procedures for documenting the claims auditing process. The President has not appointed an official claims auditor or designate an individual independent of the purchasing and disbursement processes to audit claims. In addition, the Comptroller and the Assistant Comptroller (Assistant) are responsible for approving the claims for payment and are authorized signatories on the College bank account. The Comptroller, who authorizes purchases, and the Assistant, who is involved in the disbursement process, should not audit claims because these duties are incompatible. Further, no reports are generated after a claims audit is complete to document the audit's results, including voided checks, errors identified or confirming purchase orders.[4]

College officials were unaware a claims auditor or designee should be appointed who is independent of the purchasing and disbursement processes. Without written procedures for claims processing, officials have no assurance that a proper claims audit is being performed before payments are authorized, which increases the risk that the College may overpay vendors, lose discounts or pay for goods and services not received. Without a claims audit report no documentation is available showing College officials the problems encountered, so they can be addressed and reoccurrences may be avoided.

The Board did not adopt a policy or written procedures for using or processing credit card payments as they were unaware of the importance of a credit card policy. Without a credit card policy and written procedures, there is increased risk of fraud or abuse and employees may not be accountable for damages, loss and/or improper use.

Claims Auditing Process

The audit of claims is a highly important internal control, but only if properly and effectively exercised. An effective claims auditing system ensures that tax dollars are spent appropriately by requiring a

---

[4] Confirming purchase orders are those prepared after the goods or services have already been ordered or received from a vendor, which should be limited to emergency purchases.

thorough, deliberate, and independent audit of claims before payments are authorized. All required approvals and authorizations should be documented or attached to the claim form. No claim should be paid if sufficient budgetary appropriations are unavailable and all claims should be properly authorized before payment.

Claims should contain a verified receiving slip, approved purchase order, original itemized invoice and vendor certification or department head's signed approval stating the goods or services were received and they are a true and valid charge. First and foremost, each claim must be for a legitimate purpose. The claim should be sufficiently itemized with a full description of goods or services provided. The claim should not have any sales tax charges. If the purchase was made from a State, County or other government contract, the contract number should be included on the claim.

All claims should be forwarded to the claims auditor for approval and the employee who approved the purchase should be able to provide a copy of any contract used. When feasible, vendor payments should be combined on a single voucher to reduce the costs of processing and auditing checks.

College officials need to improve the claims audit function, including the approval of credit card charges. Officials paid 12,770 claims totaling approximately $37 million during the audit period. We reviewed 75 claims totaling $104,445 and 10 credit card statements with 220 charges totaling $20,884. We found the following recordkeeping discrepancies:

- Department heads did not authorize 59 claims totaling $59,838 and 212 credit card charges totaling $19,705 before payment.

- Contracts or rates were not attached to the vouchers for 29 claims totaling $51,089 and 131 credit card charges totaling $4,647.

- Authorizations were not obtained before goods were received for 10 claims totaling $7,801 and 167 credit card charges totaling $6,657.

- Sales tax of $836 was paid on 15 credit card charges totaling $6,602.

- Supporting documentation showing whether the goods were received was missing from 14 claims totaling $6,443 and 58 credit card charges totaling $5,492.

- Rates paid for four claims totaling $3,851 did not agree with the contracts.

- Original invoices were not used to pay 36 credit card charges totaling $9,516 and five claims totaling $2,298.

- Vouchers were not sufficiently itemized for 14 credit card charges totaling $6,551 and three claims totaling $1,665.

- Purchase requisition approvals were not signed for 11 credit card charges totaling $1,546 and two claims totaling $545.

- Supporting documentation was unavailable for College officials to determine whether nine credit card charges totaling $623 were proper College purposes.

Except for nine claims, which resulted from recordkeeping errors, all the claims we reviewed were for proper purposes. However, claims were inefficiently processed because an excessive number of vouchers for the same invoice were used. Additionally, there were multiple checks issued in a single run to the same vendor. For example, one vendor was issued 478 checks totaling $57,742 for office supplies, one vendor was issued 304 checks totaling $834,052 for monthly electric utility bills and another vendor was issued 228 checks totaling $417,392 for monthly telephone bills during the 15-month audit period.

The audit of claims was ineffective because the Board did not appoint or designate an official claims auditor and College officials were not trained to audit claims. Auditing claims was also particularly difficult due to the large volume of checks issued to the same vendor on the same date.

College officials told us that vouchers are processed for each invoice to ensure vendors properly allocate the payments received because a detailed invoice breakdown is not included with the checks sent to vendors. In addition, the claims vouchers do not contain all the documentation needed to perform a thorough audit because purchase orders, purchase requisitions, quotes and contracts are maintained by the purchasing department and not compared with the vouchers before approval for payment. Incomplete voucher packages increase the risk that unauthorized purchases and services will be paid for without detection or that payments may be made at rates that do not agree with contract terms.

Recommendations

The Board should:

27. Establish written procedures for the claims process that communicates the claims auditor's responsibility and job description.

28. Formally appoint an individual who is independent of all other aspects of purchasing and the claims process to conduct a thorough audit of claims prior to approving them for payment.

29. Require the claims auditor or designee to maintain suitable records to identify what claims have been audited and whether they were allowed or disallowed, in whole or in part.

30. Adopt a credit card policy that addresses the specific circumstances under which credit cards may be used.

The claims auditor should:

31. Perform a deliberate and thorough audit of claims to ensure all claims are accurate and complete, including those for credit card charges.

The Vice President should:

32. Limit the number of checks to the same vendor on the same date within a single check run, when feasible.

33. Ensure all credit card charges are legitimate college expenses and seek reimbursement for the unsupported credit card charges identified in this report, as appropriate.

Student Accounts

The Board and College officials are responsible for establishing effective internal controls over student accounts to properly safeguard the College's assets. Effective internal controls require College officials to establish, implement and communicate policies and procedures to ensure duties are properly segregated; cash transactions are properly initiated, accurately recorded, properly approved and documented; and delinquent student accounts are enforced in a timely and consistent manner.

College officials need to improve controls in the student accounts office (office) to ensure student accounts are properly billed, collected and enforced. Any adjustments should be properly approved before being applied. Policies and procedures over student accounts were insufficient and not approved by the Board. Office staff made undocumented and unsupported adjustments to student accounts with minimal oversight. Duties within the office were not adequately segregated and College officials did not implement compensating controls, such as providing additional reviews and approvals. As a result, errors or unauthorized adjustments could be made that are undetected and uncorrected.

Generally, students were accurately billed, tuition was accurately collected and refunds were appropriately applied. However, account adjustments were made without appropriate approval and delinquent accounts were not always adequately enforced. We tested 15 student accounts with promissory notes totaling $23,155 and determined that three accounts had inaccurate amounts paid, five accounts were past due and payments for six accounts were not received in consecutive monthly installments as specified by the promissory notes. When promissory note payments are not current, the College is not receiving funds as agreed upon.

We reviewed College contracts with four collection agencies and found that the contracts were not signed by the President as required by Board policy. Contracts with two agencies were not current, one contract did not specify the timing and content of required status reports and one did not contain an updated contract for a decrease in the collection fee percentage. As a result, College officials do not have adequate assurance that the College is receiving the agreed upon collection services, is being billed the proper rate and is receiving the proper reports to monitor collection activities.

Policies and Account Adjustments

Well-designed internal controls over student accounts requires that the Board develop written policies that provide guidance for staff involved in billing, collecting, refunding and enforcing student accounts, which will enable them to understand the expectations required when performing these duties. It is important that the policies specify procedures to provide for segregating duties so one employee does not control most or all phases of a transaction and that the work of one employee is verified by another in the course of their regular duties. In instances where staff is limited, a detailed supervisory review of related activities can help ensure that policies and procedures are properly followed and that cash assets are properly accounted for, accurately reported and adequately protected.

The Board or other authorized supervisory personnel should approve all student billing adjustments and write-offs before such adjustments are made. The reasons for all adjustments should be documented and retained. Appropriate prior approval helps ensure that adjustments and write-offs are made consistently and according to College policy and reduces the opportunities for unauthorized or inappropriate adjustments.

The office is staffed by the Director and six full-time clerks, one part-time clerk and a coordinator. While the office has two refund policies, one for tuition refunds and another for financial aid refunds, the Board has not formally adopted either policy. In addition, the Board has not adopted any policies to address tuition billing, making collections, adjusting student accounts or enforcing account payments. Although the office has a procedure manual relating to tuition billing and collections, the procedures listed do not specify the job duties for each position and the expected role within the office.

College officials did not review these policies and procedures because of high turnover in key personnel. However, without sufficient student account policies and procedures, there is no formal guidance for employees to understand expectations and there is an increased risk employees may not be adequately performing their job duties.

Account Adjustments – The Director, clerk or coordinator made unsupported student account adjustments without Board or other authorized supervisory approval. College officials were unaware that adjustments should be supported and approved by someone independent from the refund and adjustment process. Without proper documentation to support an adjustment or an independent review, inappropriate adjustments could be made.

Enforcement

To ensure that the College collects all revenues, College officials must enforce the payment of past due student accounts. The status of each unpaid account should be tracked and any exceptions to the enforcement process should be documented and approved. College officials should turn unpaid accounts over to a collection agency after the College's own enforcement procedures are complete and proper authorization is obtained. Formal policies should assign responsibility and provide the details and timelines for each procedural step to be followed.

According to the College's authority for contracts policy, the President has the authority to contract for any services deemed necessary and appropriate for effective operations. The President should ensure that written agreements with collection service organizations specify the specific roles and responsibilities of each party and detail the services to be provided, including the timing, manner and cost of such services.

The College had 95 promissory notes[5] related to student accounts with original account balances totaling $201,418 as of March 15, 2017. We reviewed 15 student accounts and the related promissory notes with outstanding balances totaling $23,155.

- Five student accounts (33 percent) with balances totaling $6,058 were delinquent.

- For three student accounts (20 percent), the amount paid did not agree with the amount due on the promissory note.

- For six student accounts (40 percent) consecutive monthly payments were not received over the promissory notes' term. For example, one account a payment was not received for more than seven months.

The clerk responsible for promissory notes verifies payments are made in accordance with the agreement with minimal management oversight. If the promissory note payments are not current, the College is not receiving funds as agreed upon. Additionally without adequate oversight, delinquent accounts may not be placed into collection in a timely manner.

Collection Agency Contracts – College officials contract with four collection agencies and have 5,603 accounts in collections totaling approximately $7.8 million. During the audit period, the College paid approximately $235,000 in collection agency fees.

---

[5] Promissory notes are legal written agreements, in which students promise to pay a specified amount to the College to pay off the amounts owed on their student accounts, payable in fixed monthly installments for a set time period.

We reviewed the four collection agency contracts and found that one contract was not current (dated 2011). A second contract (from 1985) contained a 2015 addendum but not a new contract. A third agency had a new unsigned contract that did not specify when the agency will supply reports or the information the reports should contain, and the collection fee percentage was decreased by the agency via email. The President did not sign any of these contracts as required by Board policy, instead the Comptroller signed them. This occurred because the Comptroller was unaware that the President must sign all contracts.

The College's decentralized purchasing department is responsible for verifying that collection agency contracts are up-to-date and the Director maintains these agreements. Therefore, College officials were unable to ensure the contracts are regularly updated.

As a result, College officials cannot be certain the College receives the agreed upon services, is billed the proper rates and receives appropriate reports with which to monitor collection activities. In addition, if other officials sign contracts without the President's knowledge, there is no assurance that the contracts are properly entered into and in the College's best interest.

Recommendations

The Board should:

34. Establish and adopt a policy that outlines the process for maintaining student accounts.

The Director should:

35. Establish comprehensive written procedures that provide adequate guidance and internal controls over billing, collecting, refunding and enforcing student accounts.

36. Maintain proper supporting documentation for adjustments and ensure they are reviewed by someone independent from the student accounts office.

37. Ensure delinquent accounts are enforced on a timely basis.

38. Verify the accuracy and completeness of promissory notes and ensure all accounts are current or pursue additional collection activity.

The President should:

39. Review and sign all contracts and agreements deemed necessary and appropriate for effective College operations.

40. Ensure written agreements specify the College's and service provider's contractual roles and responsibilities including the timing, nature and cost of services to be provided.

The Vice President should:

41. Ensure all contracts are periodically reviewed and updated.

APPENDIX A

RESPONSE FROM COLLEGE OFFICIALS

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

September 25, 2017   **Office of the President**

Mrs. Tenneh Blamah
Chief Examiner
Office of the New York State Comptroller
Division of Local Government and School Accountability
33 Airport Center Drive, Suite 103
New Windsor, NY 12553

Re: Response to OSC Draft Audit Report

Dear Chief Blamah:

This letter is written in response to the Office of the State Comptroller (OSC) Report of Examination relating to SUNY Orange County Community College's Information Technology and Financial Activities for the period September 1, 2015 – December 1, 2016. Both SUNY Orange's Board of Trustees (BOT) and senior management team viewed this external audit of our financial practices, services, and information technology as a means to significantly improve our processes and procedures and strengthen our internal controls. In reviewing the specific recommendations presented in the report, it should be noted that there were no instances of misappropriation of funds, fraud, or wrong-doing by College personnel. Notwithstanding, we take each recommendation very seriously and commit to fully exploring every issue, and when necessary and appropriate, will implement corrective action.

The scope of the OSC Audit was broad, covering the areas of information technology, purchasing, claims, and student accounts. Although we plan to provide a formalized, detailed corrective action plan within the required timeframe, which will demonstrate clearly what corrections have already occurred or are planned, by whom and by when, this written response will provide our reaction to your findings and recommendations by area.

INFORMATION TECHNOLOGY

Board of Trustees. The Board of Trustees concur with Recommendations #1 – #4. In fact, as of November, 2016, the BOT had already formed a working subcommittee to review and update the College's policy manual.

CIO. The CIO generally concurs with Recommendations #5 - #20. However, in the corrective action plan, the CIO will respond with sufficient detail to each of the individual recommendations, describing either how the condition will be remedied, by when, and by whom or, if not to be remedied, explaining why corrective action will not be taken or perhaps what equally effective alternative action will be

115 South Street, Middletown, New York 10940 ◆ One Washington Center, Newburgh, New York 12550
phone (845) 341-4700 ◆ fax (845) 341-4998 ◆ president@sunyorange.edu

DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY   31

implemented instead. It will also be noted in the corrective action plan which recommendations have already been addressed as a result of our recent $2.8 million IT capital project that provided much needed upgrades to the Data Center and technology infrastructure on both of our campuses, providing improved data security and fail/safe improvements.

College Officials. College officials concur with Recommendation #21.

Vice President for Administration & Finance (VPAF). The VPAF concurs with Recommendation #22.

PURCHASING

Board of Trustees. The Board of Trustees concur with Recommendations #23 - #25. As previously noted, the BOT had already formed a working subcommittee to review and update the College's policy manual. This work is in progress.

Vice President for Administration & Finance. The VPAF concurs with Recommendation #26.

CLAIMS

Board of Trustees. The Board of Trustees generally concur with Recommendations #27 - #30. However, in the corrective action plan, the BOT will respond with sufficient detail to each of the individual recommendations, describing either how the condition will be remedied, by when, and by whom or, if not to be remedied, explaining why corrective action will not be taken or perhaps what equally effective alternative action will be implemented instead.

Vice President for Administration & Finance. The VPAF will address Recommendations #31 and #33 in the corrective action plan, responding with sufficient detail to both of the individual recommendations, describing either how the condition will be remedied, by when, and by whom or, if not to be remedied, explaining why corrective action will not be taken or perhaps what equally effective alternative action will be implemented instead. As for Recommendation #32, it has already been addressed. The number of checks to the same vendor on the same date within a single check run has been limited.

STUDENT ACCOUNTS

Board of Trustees. The Board of Trustees concur with Recommendation #34. As previously noted, the BOT had already formed a working subcommittee to review and update the College's policy manual. This work is in progress.

<u>Director of Student Accounts/Controller.</u> The Controller and Director of Student Accounts generally concur with Recommendations #35 - #38. However, in the corrective action plan, they will respond with sufficient detail to each of the individual recommendations, describing either how the condition will be remedied, by when, and by whom or, if not to be remedied, explaining why corrective action will not be taken or perhaps what equally effective alternative action will be implemented instead.

<u>President.</u> The President generally concurs with Recommendations #39 - #40. However, in the corrective action plan, the President will respond with sufficient detail to each of the individual recommendations, describing either how the condition will be remedied, by when, and by whom or, if not to be remedied, explaining why corrective action will not be taken or perhaps what equally effective alternative action will be implemented instead.

<u>Vice President for Administration & Finance.</u> The VPAF concurs with Recommendation #41.

Orange County Community College appreciates the cooperation and insight provided by the Office of the State Comptroller during this audit process.

Respectfully submitted,

Kristine M. Young
President
SUNY Orange
Middletown and Newburgh, NY
(845) 341-4700

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

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

- We reviewed the Board minutes, Board-adopted policies and the student accounts office procedure manual to gain an understanding of the internal controls over information technology, procurement, tuition billing, collecting, refunding, and enforcing student account payments.

- We interviewed College officials to gain an understanding of the processes and procedures over the IT system and applications, purchasing, claims, and student accounts.

- We judgmentally selected 10 employees from the business office and five employees from Student Accounts and reviewed the user permissions report for the financial software application to determine if access rights granted were based on each user's job duties.

- We reviewed all user permissions for the 10 employees with online banking rights to determine if access rights were based on each user's job duties.

- We judgmentally selected 10 employees from the business office and five employees from Student Accounts and performed an analysis on their computer web browsing histories to identify unauthorized personal Internet usage. We examined webpages visited, along with the dates and site visit times for personal, non-business, or otherwise high-risk nature webpages.

- We observed the server rooms to assess the physical controls and protection of IT assets.

- We randomly selected 10 computers and compared the serial number, tag number, and department listed on the computer equipment inventory to the actual serial number and tag number on the computer tower and what department the computer was located in.

- We judgmentally selected 10 employees from the business office and five employees from Student Accounts and compared the serial number and tag number on the computer tower to the computer equipment inventory to determine if the computers were listed on the computer equipment inventory and if the accurate department was listed.

- We judgmentally selected 25 vendors from the 69 vendors paid approximately $3.3 million and 20 vendors who provided professional services from the 34 vendors paid approximately $3.3 million during the audit period. We selected our sample based on those vendors paid an aggregate of more than $15,000 during the audit period, all collection agencies and all contracted CIO services. We reviewed these purchases to determine whether they were made in accordance with GML and the College's purchasing thresholds. We reviewed supporting documentation to determine whether the purchases made were based on objective and quantifiable analysis required for best value.

- We randomly selected 75 claims totaling $104,445 (from 12,770 claims totaling approximately $37 million) and 10 credit card statement claims totaling $20,884 paid during the audit period. We examined the claims to determine whether the purchases were properly authorized and approved before payment on an original itemized invoice, sales tax was not charged, rates paid agreed with contracts and that the purchases were for proper College purposes.

- We reviewed collection agency contracts to determine whether they were current, contained proper contract terms and contained the proper official's signature.

- We randomly selected 15 promissory notes (from 95 promissory notes outstanding) and reviewed the student account information to determine whether the account was current, the payments were accurate and payments were made throughout the note's term.

We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit 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

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

LOCAL REGIONAL OFFICE LISTING

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

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

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

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

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

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

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

Serving: Nassau and Suffolk Counties

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

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

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

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

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

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

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