THOMAS P. DiNAPOLI
COMPTROLLER

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER
110 STATE STREET
ALBANY, NEW YORK 12236

GABRIEL F DEYO
DEPUTY COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY
Tel: (518) 474-4037 Fax: (518) 486-6479

September 2015

Barbara G. Risser, Ed.D., President
Members of the Board of Trustees
Finger Lakes Community College
3325 Marvin Sands Drive
Canandaigua, NY 14424

Report Number: P2-15-10

Dear President Risser and Members of the Board of Trustees:

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

In accordance with these goals, we conducted an audit of three community colleges in western New York State. The objectives of our audit were to determine whether college officials are effectively and efficiently managing software licenses and whether security vulnerabilities exist in college websites, web applications or supporting servers. We included the Finger Lakes Community College (College) in this audit. Within the scope of this audit, we examined the policies and procedures of the College related to information technology (IT), reviewed selected computers for installed software and performed web vulnerability testing for the period September 1, 2013 through April 30, 2015. Because of the sensitivity of some of this information, we do not discuss certain results in this letter, but instead communicated them confidentially to College officials. 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 report of examination letter contains our findings and recommendations specific to the College. We discussed the findings and recommendations with College officials and considered their comments in preparing this report. The College's response is attached to this report in Appendix A. College officials generally agreed with our recommendations and indicated they planned to initiate corrective action. At the completion of our audit of the three Colleges, we prepared a global report that summarizes the significant issues we identified at all of the Colleges audited.

Summary of Findings

We found that College officials and IT staff can more effectively and efficiently manage software licenses. We found that IT staff do not maintain a comprehensive inventory list of all software that the College currently owns and the total number of licenses for each software. However, the IT staff do maintain detailed records of licenses purchased. In addition, IT staff do not regularly monitor or review computers to ensure that all software installed is appropriate and legally obtained. However, IT staff started an informal practice to review computers for installed software in late January 2015. Our detailed review of 36 computers identified one that contained a nonbusiness or nonacademic installation (golf management software). The installation of inappropriate or unlicensed software may be exposing College computers and networks to unnecessary risk, such as hacking or other malicious events.

Background and Methodology

The College is sponsored by Ontario County and operates a main campus in Canandaigua and four satellite campuses: Victor, Newark and two campus locations in Geneva. The College also provides instruction at its Muller Conservation Field Station on Honeoye Lake. The College is part of the State University of New York system and is governed by a 10-member Board of Trustees (Board) which consists of nine appointed members and a student trustee. The Board is responsible for the general management and control of the College's financial and educational affairs. The President of the College is the College's chief executive officer and the Vice President of Administrative Services is the College's chief fiscal officer. Under the direction of the Board, these individuals are responsible, along with other administrative staff, for the day-to-day management of the College.

The College has an IT department headed by the chief information officer (CIO).[1] The CIO is responsible for overseeing the College's daily IT operations and functions, including supervising IT department staff. The College also employs individuals in other IT management positions to assist the CIO in overseeing specific areas of IT operations, including a director, network and system administrators, and various coordinators. Between all campuses, the College has approximately 1,100 computers. Budgeted appropriations for IT for the 2014-15 fiscal year were approximately $2.73 million.

Software assets have become increasingly important to organizations. Not only are they a vital element of IT services that enable business-critical processes, but they also represent a large proportion of IT costs. Organizations also risk potential fines and penalties for using software applications that are not properly licensed. Additionally, organizations risk significant payroll overtime, consulting fees and equipment costs when unapproved or non-authentic software is installed on their networks, introducing unwanted, uninvited and often unintended consequences such as unforeseen crashes, breaches or system failures. Therefore, organizations need an understanding of the software they own, how it is used and how best to track user rights to ensure licensing compliance. Additionally, website and related supporting servers are also an area of significance as attackers could identify vulnerabilities and use them to their advantage

[1] The current CIO started in August 2014.

[2] Such as students, staff and faculty

to gain unauthorized access to a network, possibly exposing a network or data to security threats. Strong website and related network security could result in decreased intrusions on a system and risks associated with data breach.

Software management and website security are of particular importance to larger entities, such as colleges, that have many different users[2] that perform a variety of functions. Typically colleges will have several software applications and multiple licenses for each.

We examined installed software and licenses on College computers and website vulnerabilities for the period September 1, 2013 through April 30, 2015.[3] We interviewed College officials and staff and reviewed policies and procedures over IT to identify the controls established. We also reviewed 36 randomly selected[4] computers to determine if the installed software was appropriate and if the College had proper licenses.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results

The management of software and licenses is essential to safeguarding College assets and data. Therefore, organizations need to have an understanding of the software they own, how it is used and how best to track user rights to ensure licensing compliance. The effective management of software also includes ensuring that only appropriate business or academic software is installed to reduce the risk of unwanted consequences that could result from unauthorized software. This can be done, in part, by establishing a strong acceptable use policy, limiting users' ability to install software, regularly reviewing computers to identify installed software and taking action to remove any unauthorized software. We found that College officials and IT staff can more efficiently and effectively manage software licenses.

Software Inventory – The purpose of a software license is to grant an end user permission to use one or more copies of software in accordance with copyright law. When a software package is sold, it is generally accompanied by a license from the manufacturer that authorizes the purchaser to use a certain number of copies of the software. Organizations must obtain licenses commensurate with the number of copies in use. The implementation of a complete and comprehensive software inventory list is crucial to safeguard IT assets from potential unlicensed software being installed on computers. As a best practice, the list should include all College-owned software installed on computers and the number

[3] Specific point-in-time testing for software installations was performed on February 25 and 26, 2015. Web vulnerability testing was performed from March through April 2015.

[4] We obtained a hardware inventory list of all College computers by location and user type. We selected a total of 36 computers for review based on the following categories: student-main campus (three computers), student-satellite locations (three computers), faculty/staff-main campus (25 computers) and faculty/staff-satellite locations (five computers).

of copies currently in use. Furthermore, the list should be used in regularly reviewing all computers owned by the College to ensure that all software installed is properly approved and licensed.

We found that College IT staff do not maintain a comprehensive inventory list of all software that the College currently owns and the total number of licenses for each software. However, upon request, the IT department was able to provide records and documentation for software that would have been included on such an inventory list.[5]

In addition, IT staff did not effectively use available tools to perform regular audits of licensed software installed on computers. The College uses a software database to distribute software and control installations on individual computers. Although a report can be generated from this database detailing the total number of installations and licenses for each program, there are no formal procedures for the regular review of this report to determine licensing compliance. Additionally, the report did not include information about unlicensed programs. While the need to review individual computers for installed software is reduced because administrative rights are restricted to IT staff, there is still a risk that users could be installing unapproved or inappropriate software. However, IT staff informed us that the College purchased a software auditing tool in January 2015 to aid in monitoring licenses and installed software on computers. IT staff reviewed 11 computers in unannounced checks between January 27 and February 17, 2015. Because this tool was newly purchased, IT staff were determining the review process and, at the time of fieldwork, did not have formalized procedures for using this tool to perform regular reviews.

Because IT staff do not maintain a comprehensive software inventory list and an informal practice to review computers for installed software was not in place until late January 2015, there is an increased risk that unauthorized software was being installed and not detected. Further, the lack of regular review of software installations resulted in nonbusiness or nonacademic related software installed on a computer (golf management program).

Software Monitoring – The College developed acceptable use policies[6] to provide employees with guidelines for IT asset use and security. Computer and network resources are provided for the purpose of facilitating the academic and administrative work of employees. Specifically, employees are not allowed to download or install software without IT department approval and IT staff will perform the installation of any approved software. Furthermore, the College prohibits the installation of unlicensed or unauthorized software on computers which may result in possible copyright infringement and any installations of this nature will be removed. The acceptable use policies also identify penalties for noncompliance, which are generally defined as revocation of computer or network privileges.

College officials and IT staff have not developed formal written procedures to monitor compliance with the terms of the acceptable use policies. Therefore, to determine if installed software was authorized, had valid licenses when required, was for a legitimate business purpose and was in compliance with the College's acceptable use policies, we selected 36 computers[7] for review. We identified approximately

[5] See the Software Monitoring section for more information.

[6] Acceptable use policies adopted include Computer Devices Management and Use, Copyright Infringement Notice Takedown and Responsible Network Use.

[7] See Appendix B, Audit Methodology and Standards, for more information.

960 software installations,[8] of which 53 installations required licensing. We requested purchase orders,[9] licenses and user agreements to verify that the College had proper licensing to cover all copies of software installed on the computers reviewed. The College was able to provide supporting documentation for all installed software programs that required licensing, all of which we also found to serve a legitimate business purpose. On one computer used by a staff member, we found installed software that was not reasonable for academic or business purposes. The inappropriate software was identified as a golf management program. Based on the nature of this program, it does not serve a legitimate work-related purpose and is in violation of the College's acceptable use policies. Furthermore, non-College related programs may interfere with employees' work responsibilities.

Because IT staff did not perform regular reviews of College computers and an informal practice to review computers for installed software was not in place until late January 2015, the installation of software that is not appropriate for a business or academic purpose was not identified and a violation of the College's acceptable use policies went undetected. Potentially unauthorized software and software that does not serve a College business purpose may increase the risk that unauthorized access or modification to the computer system environment may occur, and the individual computer or network may be exposed to harmful events.

Recommendations

College officials should work with IT staff to:

1. Maintain a complete, comprehensive software inventory list of all software that the College owns and the total number of licenses for each software.

2. Formalize procedures to perform reviews of software installed on College computers and compare the results to the College's software inventory list.

3. Monitor users to ensure compliance with the acceptable use policies and ensure software installed on College computers is business and/or academic appropriate.

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 New York State 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 Secretary to the Board's office.

[8] A portion of these installations included upgrades and components of larger software programs.

[9] An effective and efficient method for purchasing and accounting for software licenses is through a purchase order system. A purchase order serves as the source document for vendor payment claims for various licenses obtained by the College and provides a record of licenses on hand to avoid duplicate purchases.

We thank the officials and staff of the Finger Lakes Community College for the courtesies and cooperation extended to our auditors during this audit.

Sincerely,

Gabriel F. Deyo
Deputy Comptroller

APPENDIX A

RESPONSE FROM COLLEGE OFFICIALS

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

Finger Lakes Community College
Office of the President
3325 Marvin Sands Drive
Canandaigua, NY 14424-8395

p: 585.785.1201
f: 585.394.5017

August 20, 2015

Edward V. Grant, Jr.
Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, NY 14614

Dear Mr. Grant,

This is to inform you that we have completed our review of the preliminary draft findings report (P2-15-10) referenced in your memo from July 16, 2015. Our Chief Information Officer, John Taylor, confirms that we agree with the findings and feels that the recommendations made are appropriate. We are also in receipt of the IT letter and agree with the recommendations therein as well.

The FLCC Board of Trustees Audit & Enterprise Risk Management Committee has also reviewed a summary of the findings and process going forward, and is in agreement with all.

We very much appreciate the opportunity this audit has given us to help improve our Information Security and Information Technology operations. We look forward to receiving your final report.

Sincerely,

Barbara G. Risser, Ed.D.
President
Finger Lakes Community College

Cc: Donna M. Mihalik, Chair, FLCC Board of Trustees
Dr. Karen Davison Blazey, Chair, FLCC Audit & Enterprise Risk Management Committee
James R. Fisher, Senior Vice President of Administration & Finance
John Taylor, Chief Information Officer
Dawn M. Hess, Director of Enterprise Risk Management

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

The objectives of our audit were to determine if College officials efficiently and effectively managed software licenses and whether security vulnerabilities exist in College websites, web applications or supporting servers. To accomplish our objective, we reviewed IT controls and processes for the period September 1, 2013 through April 30, 2015. To achieve the objectives of this audit and obtain valid audit evidence, we performed the following audit procedures:

- We interviewed College officials and staff and reviewed IT policies and procedures to determine the internal controls in place.

- We obtained a computer inventory list for all campuses from IT staff and sorted this list by location and end user (i.e., students, faculty and staff). From the inventory lists, we randomly selected 36 College-owned computers for review: 25 faculty/staff and three student computers were selected at the main campus, and five faculty/staff and three student computers were selected at the satellite campuses. We used specialized audit software to obtain a list of all software installed on each machine. We reviewed the installations for licensing requirements and to determine if they served a legitimate business purpose.

- We reviewed the provided license agreements and purchase orders to determine if the College authorized all software and whether it maintained licensing for the software installed on each of the computers reviewed.

- We reviewed the report of extracted information from the software tracking database to identify the information maintained and to determine the report's usefulness as a tool to monitor software installations.

- We reviewed the list of computers included in the College's internal software audit and inquired about the process and the results of the review with IT staff.

- We performed vulnerability testing on College websites, web applications and supporting servers using specialized scanners and audit tools.

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.