



AUDITOR GENERAL

WILLIAM O. MONROE, CPA



LAKE-SUMTER COMMUNITY COLLEGE

SELECTED INFORMATION TECHNOLOGY CONTROLS

Information Technology Audit

SUMMARY

Lake-Sumter Community College (College) uses the SCT Banner System to support various student and administrative functions. Our audit focused on evaluating general information technology (IT) controls over access to the College's computer resources, the development of an IT security awareness program, and the development and testing of a disaster recovery plan for the period July 2005 through June 2006 and selected College actions taken through January 2007; and determining the status of the College's corrective actions regarding deficiencies disclosed in audit report No. 2005-027.

The results of our audit are summarized below:

Finding No. 1: The College did not have an approved Strategic Technology Plan.

Finding No. 2: The College had not finalized a security program to ensure that exposures and vulnerabilities of IT resources had been sufficiently assessed by management and addressed through enforced user and system security controls.

Finding No. 3: Physical security and environmental controls needed improvement with regard to protection from fire and loss of power and the recording of visitor entry to the server room.

Finding No. 4: There was no written business continuity and IT disaster recovery plan.

BACKGROUND

The SCT Banner System is a comprehensive software package that is used by the College to administer student, financial aid, finance, human resources, and

payroll functions. The Student, Financial Aid, and Finance modules were implemented in 2001. The Human Resources and Payroll modules were implemented in 2002.

The Information Technologies Department was responsible for providing IT resources to meet the needs of the College. Its responsibilities included the maintenance and operation of the SCT Banner System. Headed by a Chief Information Officer (CIO) who reported to the Vice President of Administrative Services, the Information Technologies Department was organized into five groups: WebCT Support, Webmaster, Administrative Systems Management, Network/PC Support, and TV Studio Management.

Finding No. 1: Strategic Technology Plan

Senior management is responsible for developing and implementing long- and short-range plans that fulfill the organization's mission and goals and ensuring that IT issues as well as opportunities are adequately addressed and reflected in the organization's long- and short-range plans.

There was no approved strategic technology plan for the College. A draft 2004-2005 Technology Plan was never approved. College staff have indicated that the Technology Planning Committee, co-chaired by the CIO and the Dean of Business and Technologies, has developed a draft 2006-2009 Technology Plan and submitted it to the Cabinet for review. (The Cabinet

consists of the President and the three Vice Presidents.) College staff expect to have the plan completed and approved by July 1, 2007.

According to College staff, the Technology Planning Committee was given a new mission and membership roster by the President's Cabinet for the 2006-2007 academic year. The Committee, which meets monthly, is being trained to make technology decisions and to work on developing and approving plans and procedures. Without an approved technology plan, the College may not make technology decisions in its best long-term interest.

Recommendation: The College should establish an approved strategic technology plan that has both long- and short-range components.

Finding No. 2: Security Program

An entitywide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The program establishes a framework and continuing cycle of activity for assessing risk, developing and implementing cost-effective security procedures, and monitoring the effectiveness of these procedures. A sound security program helps ensure the implementation of appropriate policies and controls; promotion of security awareness; and monitoring the effectiveness of policies and controls.

The absence of a finalized information security program may have contributed to the following information security control deficiencies we noted at the College:

- The College's IT risk assessment process needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising College information. However, appropriate College personnel have been notified of these issues.
- There was no finalized security plan and various security procedures were pending approval. Although a security planning document existed, a final security plan had not been developed. According to College staff, the Technology

Planning Committee planned to begin addressing the development of a security plan before June 30, 2007. Also, various security procedures were pending approval by the Technology Planning Committee and the President's Cabinet. The College's IT department had developed IT procedures related to security, as well as other topics; however, most of these procedures were pending approval.

- The College did not have an ongoing security awareness program, which would include written policies and procedures to document such a program. Functional owners of administrative computer applications were responsible for training new users, while Human Resources provided some general new employee training. New employees also signed a statement that they had read and agreed to abide by the lists of acceptable and unacceptable uses of information systems resources. However, except for occasional e-mails warning of prevalent computer viruses, there was no ongoing security awareness program to remind users to follow good security practices to maintain the integrity, confidentiality, and availability of the College's data.
- The College did not have consistent procedures in place to ensure that access capabilities were timely removed for individuals who had terminated employment. The primary objective for timely revocation of system access privileges for identifications (IDs) belonging to terminated employees or others who do not have current need to use the College's systems is to ensure that the privileges are not exploited by the terminated employees or others. Various procedures existed within the College for the removal of user access privileges, calling for different individuals to be responsible for initiating the action. One procedure called for the department head to send an IT Help Desk request to remove network, Banner, and e-mail access from a terminating employee. Another procedure called for Human Resources to notify the security officer through e-mail requesting that the user ID be locked. According to the College, one of the termination procedures was recently revised to call for the manager of the employee to notify IT of the termination. The College plans for the Technology Planning Committee to consider whether this is the most appropriate method for IT to be notified. As demonstrated below, when inconsistent procedures exist, there is the risk that the access of terminated employees will not be timely

revoked due to confusion about who is responsible for the necessary actions.

- User IDs belonging to certain former College employees retained access to the College's systems after the employees were terminated. During our testing of access for employees who terminated employment between January 1, 2005, and September 30, 2006, we noted that user IDs for two employees retained access to the SCT Banner System for periods of 120 and 512 days after the termination dates. User IDs for two other former employees retained network access privileges for 212 and 333 days after the termination dates. In response to our audit inquiry, College staff locked (disabled) the two Banner user IDs and removed the network access for the other two user IDs. We also noted four other Banner user IDs that had already been locked, but had not been locked until 13 to 43 days after the termination dates. In the course of performing another test, we noted four additional former employees whose Banner user IDs had not been locked for from 75 to 2,170 days and one current employee whose former user ID had not been locked. A Banner consultant's user ID also had continuous access to Banner. These instances increased the risk that the terminated employees' access privileges would be misused.
- The College's access authorization practices needed improvement. An organization's written procedures for the completion of standardized system access request forms typically include provisions for indicating the type of access desired for specific data and resources; documenting management approval for both new users and users whose responsibilities have changed; and maintaining the authorizations on file. We performed a test of access authorization for 20 employees. For two employees with network access only, there was no record of a request for their network access. For three employees with Banner access, their Banner access was not approved by all relevant functional, or product, owners. For six employees, more Banner access was granted than was requested in writing, according to available records. In the course of performing the test, we noted that there were different methods of requesting access. Initial or modified access was requested via *New Hire Account Activation/Changes to Existing Account* forms, work orders, and e-mails. Inconsistent methods of requesting access increase the likelihood that the authorization records will be incomplete. College staff believe that use of a

new help desk tracking system, instituted in July 2006, will help avoid lost document issues in the future. We did, however, note that 3 of the exceptions noted previously occurred subsequent to this date. We also noted that an access request was sometimes expressed in terms of another employee's access. If the original employee terminated, his or her security profile was typically deleted from the system after a period of time. It was then difficult to evaluate whether the remaining employee was given the correct access capabilities. Of 13 Banner users tested, 8 had access requested in terms of access that had been granted to another employee. For 2 of these employees, the comparative access had already been deleted from Banner security. Without a consistent and precise method of requesting access, employees may be granted access not intended by management. Additionally, reviews of access already granted for appropriateness are more difficult if records of access approval are not complete.

- Some logon IDs were not uniquely assigned to individual persons. A unique logon ID, whether for system administrators, database administrators, or end users, provides individual identification within IT systems so that there can be accountability for actions taken. We noted that two Windows administrator IDs were used by more than one person. The capabilities for these two had not been copied to individual administrator IDs. Additionally, eight generic Banner user IDs were being used by multiple individuals. When a logon ID is not assigned to a specific individual, accountability may be lost for actions taken by someone using that ID.
- Various unused logon IDs had not been locked or deleted. Specifically, we noted two active Windows administrator IDs that were associated with software that was not currently installed at the College. In response to our audit inquiry, the College deleted these two IDs. We also found four generic Banner user IDs that were not being used but had not been locked. Of these four generic Banner user IDs, two had the database administrator role or selected sensitive system privileges. When unused logon IDs are not locked or deleted, unauthorized persons may be able to use them to view or modify the College's data.
- Certain users had been granted more access privileges than that required for the performance of their duties. A proper division of roles and responsibilities is enforced by

access control practices that exclude the possibility for a single individual to subvert a critical process and ensure that personnel are performing only those duties stipulated for their respective jobs and positions. We reviewed the appropriateness of certain Banner access capabilities for 181 Finance module users and 20 Human Resources/Payroll module users, with some overlap between the lists of users. Our review disclosed that two IT staff with database administration responsibilities had user update capabilities so that they could troubleshoot in the production database instead of the test database. Two generic Banner IDs also had update capabilities and had not been evaluated for locking. For the Finance module users, ten employees had update capabilities beyond that required for their job duties. For the Human Resources/Payroll module users, two employees had update capabilities beyond that required for their job duties. In response to our audit inquiry, College staff removed the excessive access privileges. Additionally, 24 employees in our test had been assigned access to certain screens directly rather than as part of an assigned class or standard profile, making accurate maintenance of access more complicated. In response to our audit inquiry, some direct screen access was removed for 9 employees and entire classes of inappropriate access were removed from 10 employees.

- Although the security administrator initiated selected security reviews, there was no regular review of the appropriateness of the access privileges granted to the College's Banner users. According to College staff, the College plans to establish a written security procedure, calling for a regular review of all network and Banner accounts prior to the start of each fall term. The absence of a periodic review of access privileges may have contributed to the unnecessary and excessive system access capabilities described above.
- Contrary to provisions of the Gramm-Leach-Bliley Act (GLB), the College had not established written procedures for the handling and destruction of confidential information. GLB sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These standards call for a written information security program spelling out the safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of,

or otherwise handle customer information. The applicable College policy for the handling of confidential records covered by GLB was Board Rule 2.10 (Records), which referred to Administrative Procedure PRO 2-01 (Management Information Systems). Although Board Rule 2.10 acknowledged the Board's responsibility for safekeeping, transmitting, reproducing, and destroying records and also mandates the maintenance of an information security and privacy plan, the administrative procedure referenced by the policy did not cover the identification, handling, and destruction of confidential documents. According to staff, the College has relied on personal knowledge of staff to properly handle confidential records. College staff indicated that they expect the Technology Planning Committee and the Cabinet to approve written procedures for the handling of confidential documents.

Without a well-designed information security program, responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be insufficiently or inconsistently applied. This could lead to insufficient protection of sensitive or critical resources.

Recommendation: The College should develop a written information security program. As an integral part of the program, the College should enhance its IT risk management practices to improve its ability to identify and assess IT-related risks and provide a sound basis for designing cost-effective controls to mitigate risk. As dictated through proper risk management practices, the College should establish appropriate policies, procedures, and controls to mitigate the identified risks to the extent practicable. Management should also promote security awareness through adequate training programs and develop a consistent, approved procedure for notification and removal of access privileges for terminated employees. Furthermore, management should monitor IT security, including access privileges and security events, on an ongoing basis and make appropriate changes over time to ensure the continued effectiveness of IT controls in a dynamic IT environment.

Finding No. 3:
Physical Security and Environmental Controls

Effective information security relies on a security structure that includes physical security controls that restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. Such controls include protection from fire and power outage and a record of who has had access to key computing resources.

We noted aspects of the College's physical and environmental controls over IT resources that needed improvement. Specifically:

- The main server room on the Leesburg campus had no automated fire suppression system. Instead, there was a hand-held wall-mounted fire extinguisher. Also, the uninterruptible power supply (UPS) system, which had not been upgraded as servers were added in recent years, was not under maintenance. In response to our audit inquiry, College staff indicated their plan to replace rather than upgrade the UPS system.
- Although IT staff stated that they accompanied any visitor who entered the main server room on the College's Leesburg campus, a visitor's log was not kept. Good IT physical security practices include provisions for maintaining a record of and escorting individuals who are not members of the operations group when they must enter the facilities.

The lack of adequate protection from environmental threats increased the College's risk of losing its electronic processing ability for an extended period of time. The lack of a visitor's log for the main server room may have limited the College's ability to pinpoint accountability for actions taken therein.

Recommendation: The College should consider installing an automated fire suppression system in its main server room and ensure that there is an adequate, well maintained, backup power supply for the server room contents. Additionally, the College should maintain a complete record of all visitors who enter the server room.

Finding No. 4:
Business Continuity and IT Disaster Recovery Planning

Effective disaster preparedness includes establishing a written organizationwide business continuity plan, including an IT disaster recovery plan. A good business continuity plan contains communication procedures with stakeholders, employees, critical suppliers, and management; and critical information on continuity teams, affected staff, and suppliers. It also incorporates an identification of alternatives regarding a back-up site and hardware, as well as a final alternative selection.

To ensure its ongoing effectiveness, the adequacy of a business continuity plan should be assessed on a regular basis or upon major changes to the business or IT infrastructure. This requires careful preparation, documentation, reporting of test results and, according to the results, implementing an action plan.

The College's business continuity planning needed improvement, as described below:

- There was no Collegewide business continuity plan. Although a plan had been drafted by the former CIO, College staff indicated that it needed significant revisions.
- There was no written, approved IT disaster recovery plan and no alternate processing site agreement. College staff indicated that unused servers at its South Lake campus were adequate to handle critical processing, although at a slower than usual speed; however, no testing of processing at the South Lake campus had occurred. College staff have indicated a commitment to fully implementing and testing a business continuity and disaster recovery plan by December 2007.
- The College's list of designated emergency contacts was not up-to-date. Although emergency College contacts were listed in a draft *Server Recovery (Disaster) Procedure* that was pending approval, some of the contacts were no longer with the College. According to College staff, after an IT disaster recovery plan is completed and finalized, its contents, including emergency contacts, will be reviewed annually.
- There was no contract for the supply of replacement IT equipment in the event of an

emergency. College staff stated that the reseller from which the College has obtained most of its servers has generally been responsive to the College's needs, but a contract for the supply of critical equipment in an emergency will be considered during the IT disaster recovery plan rewrite.

Without a written and tested business continuity and disaster recovery plan, the College may not be able to resume critical processing within an acceptable period of time following a disaster that renders its normal processing facility unusable.

Recommendation: The College should prepare, and periodically test, a business continuity and disaster recovery plan that will enable it to timely resume processing in the event of a disaster.

PRIOR AUDIT FINDINGS

The College had corrected, or was in the process of correcting, deficiencies noted in audit report No. 2005-027, with the exception of issues noted in Finding No. 2 above.

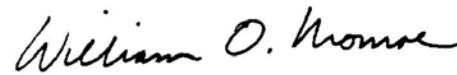
OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected general IT controls over access to the College's computer resources, the development of an IT security awareness program, and the development and testing of a disaster recovery plan. We also focused on determining whether management had corrected, or was in the process of

correcting, the deficiencies disclosed in audit report No. 2005-027 during the period July 2005 through June 2006, and selected actions taken through January 2007, including a risk assessment and security program, controls over access to programs and data, and network operating controls. In conducting our audit, we interviewed appropriate College personnel, observed College processes and procedures, and performed various other audit procedures to test selected IT controls.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our information technology audit.



William O. Monroe, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated May 3, 2007, the College provided responses to our preliminary and tentative findings. This letter is included at the end of this report as Appendix A.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was conducted in accordance with applicable Generally Accepted Government Auditing Standards. This audit was conducted by Sue Graham, CPA*, CISA, and supervised by Nancy Reeder, CPA*, CISA. Please address inquiries regarding this report to Jon Ingram, CPA*, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (<http://www.state.fl.us/audgen>); by telephone (850 487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida.

APPENDIX A
MANAGEMENT RESPONSE



May 3, 2007

Mr. William O. Monroe, CPA
Auditor General
State of Florida
G 74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Monroe,

The attached is Lake-Sumter Community College's response to the preliminary and tentative findings and recommendations pertaining to the Information Technology Audit of Lake-Sumter Community College for the period of July 2005 through June 2006 and selected College actions through January 2007.

Should you have any questions on any of our responses please don't hesitate to contact me at 352-365-3525.

Sincerely,

A handwritten signature in cursive script that reads "Richard M. Scott".

Richard M. Scott
Vice President of Administrative Services
Lake-Sumter Community College

RMS/lga

Cc: Charles R. Mojock, Ed.D.
Brenda Racis
John Froman

Attachment

LEESBURG CAMPUS
9501 U.S. Hwy. 441, Leesburg, FL 34788
352-787-3747 • FAX: 352-365-3501

SOUTH LAKE CAMPUS
1250 N. Hancock Rd., Clermont, FL 34711
352-243-5722 • FAX: 352-243-0117

SUMTER CAMPUS
1405 C.R. 526A, Sumterville, FL 33585
352-568-0001 • FAX: 352-568-7515

Lake-Sumter Community College Information Technology Audit - Findings and Responses

Finding No. 1: The College did not have an approved Strategic Technology Plan.

Response: The College has a draft Strategic Technology Plan that has been presented to the College Cabinet. This draft plan has been sent back to Technology Committee for further refinements and final adjustments. It is expected that the College will have an approved Strategic Technology Plan within the next 120 days.

Finding No. 2: The College had not finalized a security program to ensure that exposures and vulnerabilities of IT resources had been sufficiently assessed by management and addressed through enforced user and system security controls.

Response: The College agrees with the need to improve and finalize all elements of an overall security program. The College has already addressed and made modifications to a number of key components within its security plan including Access Control and Auditing, Risk Assessment/Review and Security Awareness.

This recent audit has brought a renewed focus to several areas of security which will be addressed in the College's new comprehensive security plan. These efforts to enhance and strengthen security will need to be ongoing and updated frequently as changes in technology risks are not static.

Finding No. 3: Physical security and environmental controls needed improvement with regard to protection from fire and loss of power and the recording of visitor entry to the server room.

Response: The College agrees that enhanced fire protection and power backup are needed improvements. In the meantime, all battery backup units have been replaced while the College plans for a new technology area which will have automated fire suppression and better emergency power generation. Access to the server room has already been changed and a new login process is now in place for the server room.

Finding No. 4: There was no written business continuity and IT disaster recovery plan.

Response: The College agrees that a documented and functional Business Continuity and IT Disaster Recovery Plan should be put in place. Many of the elements of such a plan are already in effect but need to be properly documented and placed in the Plan. The formal Business Continuity and IT Disaster Recovery Plan will be developed and adopted by December, 2007.