



AUDITOR GENERAL

WILLIAM O. MONROE, CPA



LAKE-SUMTER COMMUNITY COLLEGE

SCT BANNER SYSTEM PAYROLL MODULE

Information Technology Audit

SUMMARY

Lake-Sumter Community College (College) uses the SCT Banner System to support various student and administrative functions. The SCT Banner System operates in a client server environment.

Our audit focused on the Payroll module of the SCT Banner System, as implemented by the College. We also evaluated selected general controls within the overall information technology (IT) environment of the College for the period February 2004 through May 2004, and selected College actions taken from June 2000, and determined management’s awareness of and actions taken regarding the Health Insurance Portability and Accountability Act (HIPAA).

As described below, we noted deficiencies in certain controls related to the College’s IT functions and practices.

Finding No. 1: The College had not developed a Collegewide 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. Additionally, during our field work, the College had not established a security management structure with a central figure (Information Security Manager or similar function) assigned the responsibility of overseeing the security program.

Finding No. 2: Operational deficiencies were noted in the College’s security controls within the SCT Banner application environment.

Finding No. 3: Deficiencies were noted within the security of the network operating environment at the College.

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 during Summer 2001. The Human Resources and Payroll modules were implemented in January 2002. The College used the system as delivered by the vendor without in-house modifications to the base system code.

**Finding No. 1:
Collegewide 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. Principles that help ensure that information security policies address current risks include a sound IT risk management process to identify, assess, and mitigate risks; establishment of a central management focal point, implementation of appropriate policies and controls, promoting security

awareness, and monitoring the effectiveness of the policies and controls.

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

- The College's IT risk management 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.
- During our field work, the College had not formally designated an Information Security Manager to serve as a unification point for all of the College's security issues. Although the College had designated a Security Administrator who was responsible for communicating security procedures with faculty, staff, and students, it had not formally established a structure to implement a Collegewide security program nor had the responsibilities of a central security manager been defined. However, subsequent to our field work, the College named an Information Security Officer (ISO) and began work on overall information security at the College.
- The College did not have a security awareness training program. Additionally, College requirements for user acknowledgement of security responsibilities were not being followed. Contrary to Board of Trustees rules¹ and College administrative procedures², the College did not, prior to granting users access to IT resources, require the users to sign forms acknowledging that they had read and agreed to abide by the Board's rules for acceptable use of IT resources. For a security plan to be effective, those expected to comply with it need to be aware of it. Without an adequate security awareness and training program, the risk is increased that users may not be aware of their security responsibilities.
- The College did not have adequate policies and procedures in place to ensure that access capabilities were timely revoked or modified, as necessary, for individuals who had

terminated employment. The primary objective for timely revocation of system access privileges for terminated employees is to ensure that privileges are not exploited by the terminated employee or others. During our testing of user access for employees who terminated employment between January 2003 and March 2004, we noted that user IDs for 14 employees retained access to the SCT Banner System after the termination dates. One of these employees also had an active network account. In a separate test of employee access rights, we noted an additional 15 user IDs of employees who had terminated prior to January 2003 and also retained access rights to the SCT Banner System. The College indicated that it had a formal procedure in place whereby the Department head and the personnel office notified the appropriate security coordinator to remove SCT Banner System access and network access; however, the procedure had not been followed on a consistent basis. Once notified of our test results, the College removed the terminated employees' access. The College was unable to provide access logs indicating if any of the terminated individuals had logged onto the system after termination and prior to the account being deactivated. Without adequate procedures to ensure the timely revocation of access privileges of terminated personnel, the risk is increased of unauthorized access to the College's information resources.

- Access authorization documentation approving user access to the network and the SCT Banner System was not maintained for all users. During our test of access authorizations, we noted that the College did not maintain supporting documentation for the access granted to the network or SCT Banner System for 11 of 15 employees tested. We also noted one instance where the authorization documentation did not match the actual level of access which had been granted. When access is not limited to what is authorized and approved by management, the risk is increased of unauthorized use of information resources.
- The College did not maintain documented procedures to address the handling of electronic or hardcopy confidential records covered by Federal privacy legislation in the

¹ Board of Trustee Rule 2.16

² Administrative Procedure 7-16

Gramm-Leach-Bliley Act (GLBA)³, such as names, social security numbers, and bank account information associated with student loans, and employee financial information. Pursuant to a Federal Trade Commission rule⁴ implementing the GLBA, the College is required to develop, implement, and maintain a comprehensive information security program. The rule further specifies required elements of an information security program. While the College maintained a policy to govern confidential information, it lacked the supporting procedures to ensure protection of confidential student and employee financial information. Absent formal procedures for handling confidential records, the risk is increased of unauthorized disclosure of that information.

- Management had not established adequate policies and procedures for the periodic review of user access rights and the monitoring of security events. We noted that the College did not perform periodic reviews of user access granted to the SCT Banner System. Additionally, we noted that the College did not maintain procedures to periodically review the security groups and permissions granted within the Windows network.

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 formal 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. The newly named ISO should function as management’s central focal point to

³ Public Law 106-102

⁴ Title 16, Part 314, Code of Federal Regulations (2002)

oversee the program. The ISO’s duties and responsibilities should be well defined. Management should also promote security awareness through adequate training programs. 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. 2:
Operational Security Controls**

Effective information security relies on a security structure that includes operational procedures, organization, and resources. We noted deficiencies in the College’s operational security controls in the areas of user identification and authentication, management of access privileges, monitoring of security activity, and physical access to the data center. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising College information. However, appropriate College personnel have been notified of the deficiencies.

Recommendation: The College should strengthen its security controls in the above-listed areas.

**Finding No. 3:
Network Security Controls**

Network security controls are intended to reduce the risk of intrusion to the IT network and the misuse of data and network resources. We noted the following deficiencies within the network environment at the College:

- The College had not developed written policies and procedures for the control of new technologies that provide additional network connections within the IT environment. Specifically, the use of Personal Digital Assistants (PDAs), wireless devices, and Instant Messaging (IM) utilizing the Internet had not been addressed. Although the IT Department supported PDAs by selected administrative staff; planned to roll out a wireless network for administrative and

student access; and permitted the use of IM on client machines connected to the College’s network, written policies and procedures were not maintained to guide users in appropriate use of these technologies. Absent policies and procedures on the use and installation of these technologies, the risk of unauthorized network access and the introduction of malicious software is increased.

- We noted certain technical deficiencies in the network security controls maintained by the College. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising the College’s information. However, appropriate College personnel have been notified of these deficiencies.

Recommendation: The College should enhance its network security controls in the above-mentioned areas.

OTHER MATTERS

**Health Insurance Portability and
Accountability Act of 1996
(HIPAA)**

HIPAA⁵ addresses data interchange, privacy, and information security standards for personal health information. Pursuant to HIPAA, the United States Department of Health and Human Services has published regulations on electronic data interchange standards, privacy, and security. The final Transaction Rule, which contains electronic data interchange standards, was incorporated as a Federal regulation and had a compliance date of October 16, 2002. The final Privacy Rule was incorporated as a Federal regulation and compliance was required by April 14, 2003. The final Security Rule was incorporated as Federal regulation and has a compliance date of April 21, 2005. HIPAA also provides for civil and criminal penalties for noncompliance.

Management determined that the College did not engage in covered HIPAA transactions or activities requiring compliance with either the Transaction Rule or Security Rule. However, management determined that the College was subject to the Privacy Rule because employee health information was handled through the personnel office. The College indicated that, in accordance with the rule, it had designated a Privacy Officer, distributed Notices of Privacy Practices, developed and documented policies and procedures, and conducted training of appropriate personnel. The College further noted that it would continue to monitor its activities related to protected health information and, in the event circumstances change, take necessary steps to ensure compliance.

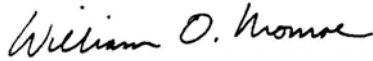
OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected College IT controls and to determine management’s awareness of and actions taken regarding the HIPAA legislation. Our scope focused on evaluating internal controls and selected IT functions applicable to the Payroll Module of the SCT Banner System during the period February 2004 through May 2004, and selected College actions taken from June 2000. 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.

⁵ Public Law 104-191

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

AUDITEE RESPONSE

In a letter dated September 2, 2004, the President provided responses to our preliminary and tentative findings. This letter is included in its entirety at the end of this report.

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 made in accordance with applicable standards contained in *Government Auditing Standards* issued by the Comptroller General of the United States. This audit was conducted by George Allbritton, 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.

Lake Sumter

COMMUNITY COLLEGE
Office of the President • Dr. Charles R. Mojock

September 2, 2004

Mr. William O. Monroe, CPA
Auditor General, State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Sir:

Enclosed please find the Lake-Sumter Community College response to the Information Technology Audit dated August 5, 2004. While we were satisfied with the acceptable review of most aspects of our security, let me assure you that the College takes the findings and recommendations very seriously. As you will see in the response, we have initiated corrective actions to address the concerns raised by the audit.

We appreciated the professionalism and courtesy of the staff involved in the audit. Thank you for your assistance in helping us ensure the integrity of these critical systems.

Sincerely,



Charles R. Mojock, Ed. D.
President

cc: Mr. Dick Scott
Mr. Bill Campman

LEESBURG CAMPUS
9501 U.S. Highway 441
Leesburg, Florida 34788-8751
(352) 787-3747

SOUTH LAKE CAMPUS
1250 N. Hancock Road
Clermont, Florida 34711
(352) 243-5722

SUMTER CAMPUS
1405 C.R. 526A
Sumterville, Florida 33585
(352) 568-0001

Lake-Sumter Community College
Response to Auditor General
SCT Banner System Payroll Module Audit Recommendations

Finding No. 1:

Collegewide Security Program

The College had not developed a Collegewide 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. Additionally, during our field work, the College had not established a security management structure with a central figure (Information Security Manager or similar function) assigned the responsibility of overseeing the security program.

Response:

The college IT staff and the Vice-President of Administrative Services have reviewed the recommendations in the published and confidential report and steps are underway to address each of the findings. We agree that a strong information security plan along with proper education is very important. We plan on instituting a comprehensive IT risk management plan in place by December 1, 2004 to be followed by appropriate employee awareness training underway.

Information Security Program Highlights:

1. The appointed security officer, the Vice-President of Administrative services, has met with a small group of directors to begin the security awareness and security information policy improvement process. This committee also has the charge to ensure compliance with all state and federal mandates regarding information security (electronic or paper). This information will become the employee education program. This committee will also determine the need and recommend budget for additional security practices including such items as: additional security software, security review practices, and the need for additional risk assessments.
2. A sub-committee of the Technology Planning Committee has been tasked with addressing specific technical security practices and associated policy creation. This committee will provide more of the detailed information for security controls, monitoring systems, password parameters, and desktop policies.
3. The IT department has been allocated an IT training position with duties assigned to promote security awareness and provide proper education for all faculty and staff. A new information portal is in design with a section of this portal to be dedicated to information security.
4. A new procedure has been implemented through human resources which notifies the IT staff of all employee termination in a timely manner. Additionally, a procedure has been drafted

to transfer appropriate data and e-mail access from terminated employees to current employees. This will allow business continuity once the employee is terminated. The IT department and the ISO will be working with the HR department to provide regular staff training on information security.

5. A functional user committee under the direction of IT is working to identify standard user templates for all Banner functions. These templates will be implemented based on job descriptions with appropriate user access assigned. This will cause a complete re-evaluation of all employee access to the Banner information system.

6. IT staff will be provided with access to appropriate education opportunities to strengthen knowledge in areas of security. Through seminars, course materials and attending formal training IT staff will have the advantage of exposure to material to better address security practices and information security policies.

Finding No.2:

Operational deficiencies were noted in the College's security controls within the SCT Banner application environment.

Response:

The items mentioned in the report are being addressed by the comprehensive security plan in the response to finding 1.

Finding No.3:

Deficiencies were noted within the security of the network operating environment at the College.

Response:

The Technology Committee is charged with defining procedures and policies for all new technology contained in the technology plan including procedures for wireless, PDA's, and IM. The wireless network will not be implemented until the policies are in place. The Technology Committee will address a usage policy for IM and PDA's. The IT department has purchased and is installing virus protection for all PDA's in use.

We greatly appreciate the thorough review provided to LSCC through the Information Technology Audit. The audit staff was both helpful and professional.