AUDITOR GENERAL

WILLIAM O. MONROE, CPA

FLORIDA ATLANTIC UNIVERSITY
SCT BANNER SYSTEM PAYROLL MODULE

Information Technology Audit

SUMMARY

Florida Atlantic University is a public university with multiple campuses in south Florida. The University uses the SCT Banner enterprise resource planning (ERP) software for both its human resource management and financial management applications. SCT Banner operates in an Internet-based environment supported by the Information Resource Management (IRM) department at the University. IRM is organizationally placed under the Associate Provost and Chief Information Officer and is located within the computing center at the main campus in Boca Raton.

Our audit focused on evaluating selected application controls related to the SCT Banner System Payroll Module, as implemented by the University, and selected general controls within the overall information technology (IT) environment applicable to the University for the period February 2005 through May 2005. We also evaluated University actions taken in response to selected IT-related deficiencies noted in audit report No. 2004-013.

As described below, we noted deficiencies in certain controls related to the University's functions and practices.

Finding No. 1: The University had not developed an entitywide 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 University 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: Deficiencies were noted in the University's access security controls within the SCT Banner application environment.

Finding No. 3: Improvements were needed in certain security controls within the overall operations of the application and the supporting network environment at the University.

BACKGROUND

The University transitioned from the State's financial accounting system, the Florida Accounting Information Resource Subsystem (FLAIR), to the SCT Banner System, which is a comprehensive software package that includes modules to administer student, financial aid, finance, human resources, and payroll functions. The SCT Banner finance module was implemented on July 1, 2003, and the human

resources/payroll module was implemented on January 1, 2004. The student and financial aid modules operated in a mainframe environment supported by the North West Regional Data Center; however, the University planned to move the student system modules to the University's data center in October 2006. The University used the system as delivered by the vendor without in-house modifications to the base system code.

Finding No. 1:
University 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 effective security procedures, and monitoring the effectiveness of these procedures. Principles that help ensure that information security policies address current risks include performing a periodic risk assessment to determine needs; establishing a central management focal point; implementing appropriate security policies and controls to mitigate identified risks; promoting security awareness; and monitoring the effectiveness of the policies and controls.

Certain deficiencies were noted within the overall University security program as follows:

- The University had not performed a formal risk assessment. Although the University had informally analyzed risks regarding its IT resources and implemented informal procedures to mitigate these risks, management had not documented this analysis and had not consistently documented management decisions in the form of written policies and procedures established to mitigate risks to the physical and logical access security of the University's IT resources.
- During our field work, the University had not formally designated an overall Information Security Manager to serve as a unification point for all of the University's security issues. Although the University had designated an Application Security Coordinator and a Network Security Coordinator, neither had the authority to make policy decisions at the Universitywide level, nor had a structure to implement a security program at that level been defined.
- The University had not developed an adequate security awareness training program. Although the University Web site addresses security awareness, there was no mechanism to ensure that employees read the security awareness guidance or agreed to adhere to it. In addition, there was not a process to facilitate ongoing security awareness training.
- The University did not have adequate written security policies and procedures in place to control the following:
  - Approving, granting, and removing access to the SCT Banner application.
  - Periodic review of the SCT Banner user access accounts.

- Monitoring of the SCT Banner application and database security events.
- SCT Banner database administration procedures.
- Approving, granting, and removing access to the data center.

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

Recommendation: The University should develop a formal entitywide security program. A risk assessment should be the starting point for identifying risks and determining the University's needs. A Universitywide Information Security Manager (ISM) should be established and should function as management's central focal point to oversee the program. The ISM's duties and responsibilities should be well defined. Appropriate policies, procedures, and controls should be implemented to mitigate the identified risks. Management should also promote security awareness through adequate training programs. Furthermore, management, on an ongoing basis, should monitor the effectiveness of the IT environment, the security program, and specific security controls, and make changes as needed.

Finding No. 2: Application Access Control Procedures

Access controls are intended to protect data and IT resources from unauthorized disclosure, modification, or loss. We noted certain deficiencies in the University's access control procedures related to the SCT Banner application, as described below:

- Authorization of access to the University's SCT Banner application had not been properly documented for all users. Good access controls include instituting policies and procedures for authorizing access to information resources, documenting such authorizations, and then periodically monitoring actual access capabilities through comparisons to the authorizations. Of 19 access authorizations tested, we noted 3 instances where proper access documentation was not maintained and 14 instances where the authorization documentation did not match the actual level of access that had been granted. When access is not limited to what is authorized and approved by management, the risk is increased of inappropriate use of information resources.
- The University 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. During our testing of user access for employees who had terminated employment between January 2004 and February 2005, we noted that SCT Banner application access privileges were not timely revoked for two terminated employees. Specifically, the SCT Banner accounts were deleted 26 and 121 days, respectively, after the employees' termination dates. In response to our inquiries, the University indicated that it had previously implemented informal procedures whereby the Assistant Director of Personnel Services runs bi-weekly reports and then notifies the appropriate security coordinator to remove SCT Banner application access; however, these procedures were implemented after the two above-noted employees had terminated. The University was unable to provide access logs indicating whether the terminated individuals had logged on to 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 for unauthorized access to the University's information resources.

- Our audit disclosed instances of inappropriate or unnecessary access privileges. An appropriate division of roles and responsibilities excludes the possibility for a single individual to subvert a critical process. When enforced through appropriate system access privileges, such a division helps ensure that personnel are performing only those duties stipulated for their respective jobs and positions. During our testing of access privileges for an appropriate segregation of duties, we noted the following:

  - Seven instances in which employees appeared to have inappropriate access to the SCT Banner finance-related functions.
  - Two instances where an SCT Banner-delivered user account (ID) appeared to have inappropriate SCT Banner finance-related functions. SCT Banner-delivered user IDs are generic accounts that are implemented with the application.
  - Two instances where user IDs had direct and unnecessary access to sensitive SCT Banner objects, which allowed the users to perform incompatible accounting functions. Objects define the fields which can be entered on an input screen.
  - Nineteen instances where user IDs appeared to have inappropriate access to SCT Banner human resource/payroll functions. Eleven of these 19 instances were SCT Banner-delivered user IDs.

  Absent appropriate segregation of duties, the risk is increased that erroneous or fraudulent transactions could be processed and that computer resources could be damaged or destroyed.

- The University did not monitor SCT Banner application security events. Appropriate IT security administration ensures that security activity is logged and any indication of imminent security violation is reported immediately. Both the SCT Banner application and the Oracle database had logging options (audit trails) enabled; however, the University did not have procedures established to routinely monitor the logs. Without routine logging and monitoring, the risk is increased that unauthorized access or changes could be made and not detected in a timely manner.

Recommendation: The University should strengthen its access control procedures including documenting access authorizations, reviewing the ongoing appropriateness of access privileges, and monitoring significant security events.

Finding No. 3:
Operational Security Controls

Physical and logical controls are established to protect data files, application programs, and hardware. In a networked environment, it is important to identify and protect all the entry points and paths to sensitive files. We noted the following deficiencies within the SCT Banner application and supporting network environment.

- The University had not developed written policies and procedures for the control of many of its IT functions within the SCT Banner application and the supporting network environment. We noted that informal procedures were utilized in the following areas:

- Development of external programs and procedures using SCT Banner data.
- Maintenance and monitoring of the operating system, intrusion detection system, virus software, firewall, and other network equipment.
- Removal of data from surplus equipment.
- Use of wireless devices that connect to the network.

Without formal policies and procedures outlining controls and measures necessary for the quality and consistency with which an entity's objectives are achieved, management may not have a sufficient basis for determining whether directives are properly performed and personnel may not have sufficient guidelines for meeting management's expectations.

- Although the University maintained a written business continuity plan, we determined that the plan lacked some necessary information, including:
  - Proper level of instruction to employees in the event of an emergency
  - Proper contact information for staff members and vendors
  - Instructions for recovery from a disaster
  - Instructions for remote operations
  - Which computing functions to be restored in off-site locations

  Although the University tested part of the business continuity plan utilizing the payroll application, the full plan had not been tested nor had a system of periodic testing of off-site alternate locations been implemented. Without a complete and tested recovery plan, management risks not being able to timely and effectively recover its IT resources should a disaster occur.

- We noted the following deficiencies in the data center's physical controls over the computer room:
  - One University employee, who had terminated on December 9, 2004, still had swipe card access to the data center as of January 31, 2005.
  - Computing equipment could be viewed through a glass window from outside the data center.
  - The room housing the routers and Uninterruptible Power Supply did not have a raised floor, leaving the equipment susceptible to water damage.
  - The data center has a "dry" pipe fire suppression system in place. We noted pipes directly over the Sun servers and, if the system was activated during a fire, the servers would be damaged by water.

  Without having appropriate physical controls in place to adequately restrict access to the computer room, the risk of losses due to human error and abuses is increased. Without adequate environmental controls, the risk is increased that the University cannot prevent or minimize the damage to automated operations that can occur from unexpected events.

- We noted certain other deficiencies within the SCT Banner environment related to technical security controls. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising University information. However, appropriate University personnel have been notified of these deficiencies.

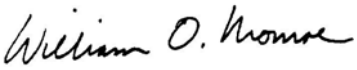
Recommendation: The University should develop the appropriate policies and procedures as noted above and complete the documentation and testing of the business continuity plan. Also, termination procedures should be strengthened, including removing employee swipe card access to the data center. Additionally, since the University has indicated that it plans to renovate the data center, it should address the other physical control deficiencies identified above as part of the renovations.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected University controls and to determine actions management has taken to correct IT-related deficiencies disclosed in audit report No. 2004-13. 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 2005 through May 2005. In conducting our audit, we interviewed appropriate University personnel, observed University 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

AUDITEE RESPONSE

In a letter dated August 30, 2005, the University 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 Bill 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.

FAU
FLORIDA ATLANTIC UNIVERSITY

Office of the Vice President for Financial Affairs
777 Glades Road
Boca Raton, FL 33431
tel: 561.297.3266 / fax: 561.297.2772
jessell@fau.edu
www.fau.edu/admin/fiscal

August 30, 2005

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

Dear Mr. Monroe:

In connection with the Florida Atlantic University Information Technology audit, enclosed are Florida Atlantic University's responses to the preliminary and tentative audit findings. Under separate cover, Florida Atlantic University is transmitting the confidential documents that complete the University's responses.

Should you have any questions or need additional information, please don't hesitate to call me at 561-297-3267.

Sincerely,

Kenneth A. Jessell, Ph.D.
Vice President for Financial Affairs

KAJ/lae

Attachment

cc: President Frank Brogan
Dr. Jeffrey Schilit
Mr. Dennis Crudele

Information Technology Audit of the
Florida Atlantic University,
SCT Banner System Payroll Module
for the period February 2005 through May 2005

PRELIMINARY & TENTATIVE AUDIT RECOMMENDATIONS & RESPONSES

Recommendation: *The University should develop a formal entity wide security program. A risk assessment should be the starting point for identifying risks and determining the University's needs. A University wide Information Security Manager (ISM) should be established and should function as management's central focal point to oversee the program. The ISM's duties and responsibilities should be well defined. Appropriate policies, procedures, and controls should be implemented to mitigate the identified risks. Management should also promote security awareness through adequate training programs. Furthermore, management, on an ongoing basis, should monitor the effectiveness of the IT environment, the security program, and specific security controls, and make changes as needed.*

Response:

On February 15, 2005, Information Resource Management (IRM) in conjunction with Personnel Services began distributing to its new employees as part of their orientation, a new publication entitled "Information Technology Password and Security Awareness Guide." Additionally, IRM has developed a special issue of the IRM Newsletter (September 2005) dedicated exclusively to address IT security "Best Practices" as well as to inform the user community about common threats and security risks to the Internet and desktop software packages.

IRM has reinstated the university-wide technology security committee, Security and Network Awareness Group (SNAG). SNAG will meet four times per year to promote IT security and recommend policies and actions to the Associate Provost and Chief Information Officer to better protect the distributed information technology infrastructure of Florida Atlantic University. Membership includes representatives from all FAU Colleges, the University Police Department, the Inspector General's Office, a representative of each partner campus. Administration, and IRM.

Florida Atlantic University is currently reviewing all policies and procedures governing Banner FR/HR application security and control. IRM and the functional areas have implemented changes limiting access to the production environment, tables, and data files. Changes include actions such as requiring all staff to complete a FAU Position of Trust security form, signing a BANNER security form and reevaluating who should have access to controlled data fields.

Several FAU employees were active participants of a Miami Electronic Crime Taskforce Seminar hosted by the United State Secret Service. Publications, resources, and educational activities from this Taskforce to promote security awareness have been shared with the members of the university technology staff.

Information Resource Management filled the position of Network Security Officer over two years ago. A Banner and Oracle Application Security Officer was also appointed at that time. The University is again reviewing the possibility of filling the Chief Security Officer position. Due to funding, this position was never filled but the responsibilities were assumed internally by IRM. The position will be advertised, contingent upon adequate funding, from the 2006-07 budget cycle.

Recommendation: *The University should strengthen its access control procedures including documenting access authorizations, reviewing the ongoing appropriateness of access privileges, and monitoring significant security events.*

Response:

In order to better track utility programs, networking devices, and applications on systems deemed critical, the University has created additional logs. IRM has strengthened its internal policy so that all system security logs will be reviewed on a daily basis by the system administrator. In addition, IRM has filled a new position whose responsibilities are to review networking logs on a daily basis.

Banner application security, audit logs, and access control logs are now reviewed on a weekly basis by the Director of University Administrative Systems, as well as, each functional area security officer. Procedures and processes have been established so that the Oracle database activity logs will be viewed on a daily basis by the Director of University Administrative Systems. These logs are kept in a secure system and functional area security officers have been given access only to tables related to their area of responsibility. Appropriate procedures to outline database administrator activities have been developed and set forth on May 17, 2005.

Information Resource Management in conjunction with Financial Affairs Application Security Officers, have established a procedure to better monitor access to Banner FR/HR and the Student Information System (currently under implementation) databases. This stringent security practice requires that all direct access to the Banner tables be approved by area directors as well as the authorized data file administrator/owner.

An access control form has been developed and all FAU employees, including software developers, database administrators, and application coordinators requiring access to the Banner tables both in the production and test regions, must complete this Security and Access Control Form with the stipulation that access may be revoked at any time. These forms are subject to annual renewal.

Recommendation: *The University should develop the appropriate policies and procedures as noted above and complete the documentation and testing of the business continuity plan. Also, termination procedures should be strengthened, including removing employee swipe card access to the data center. Additionally, since the University has indicated that it plans to renovate the data center, it should address the other physical control deficiencies identified above as part of the renovations.*

Response:

On May 18, 2005, Information Resource Management updated and submitted to the Office of Environmental Health and Safety (EH&S) it's Continuity of Operations Plan (COOP). This document is based on the general guidelines established by EH&S.

IRM also updated its Building Emergency Contingency Plan in June 2005. This document addresses the action plan in the event of natural disasters. These plans give instructions and the necessary steps for providing order of succession as well as the procedure for enacting the

emergency plan by the University President or his/her designee. These plans supersede the plans previously sent to the State Auditor's Office.

IRM is currently developing a comprehensive risk assessment and mitigation plan. This plan is being developed using guidelines established by the National Institute of Standards and Technology (NIST). The anticipated completion of this plan is September 2005 and the plan will be forwarded to the State Auditor's Office.

IRM is scheduled to deliver secure and encrypted wireless access to the University community on September 1, 2005. In conjunction with IRM, the Personnel Services Department has simplified the employee termination process to more fully integrate into the Banner System. This new process was updated and implemented on May 17, 2005.

The renovation of Florida Atlantic University's Data Center is now scheduled for completion in May 2007. Several critical physical control deficiencies in the IRM Data Center have been discussed with the awarded architectural firm, PGAL, which will be integrated into the final building plans such as, raised floors in the operations room and a dry pipe flame suppressant system in the operations room.

4

THIS PAGE INTENTIONALLY LEFT BLANK