FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

AUDIT OF THE CONTROLS OVER ATHLETICS TICKET REVENUE

Report No. 10/11-07

February 3, 2011

FIU | FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

Date: February 3, 2011

To: Mark Rosenberg, University President
Pete Garcia, Athletic Director

From: Allen Vann, Audit Director

Subject: **Audit Report of the Controls Over Athletics Ticket Revenue**
Report # 10/11-07

We have completed an audit of the controls over athletics ticket revenue for all University sporting events. The primary objective of our audit was to determine whether established controls and procedures are adequate; are being adhered to; and are in compliance with University policies and procedures, and applicable state statutes, rules and regulations. As part of the audit, the controls over the information systems used in the ticketing process were also examined.

Overall, except for certain controls requiring additional strengthening, the Athletics Department's procedures for the sale of tickets are generally adequate. Processes that management agreed to improve include: prompter deposits, employee background checks, segregation of duties, and ticket sales report reconciliations. There were also security control deficiencies in the sales information systems that required attention. In all, the audit resulted in 23 recommendations, which management agreed to implement.

We again wish to express our appreciation for the cooperation and courtesies extended to us by the Athletics Department while conducting the audit.

C: Albert Maury, Chair, and Members of the Finance and Audit Committee
Kenneth Jessell, Chief Financial Officer and Senior Vice President
Javier I. Marques, Chief of Staff, Office of the President
Alex Duque, Associate Vice President, Athletics
Heath Glick, Chief of Staff, Athletics
Jeremy Lamb, Assistant Ticket Sales Manager, Athletics

TABLE OF CONTENTS

OBJECTIVES, SCOPE, AND METHODOLOGY

The primary objective of our audit was to determine whether established controls and procedures over the Athletics Department's revenues generated from athletic event ticket sales are adequate; are being adhered to; and are in compliance with University policies and procedures, and applicable state statutes, rules and regulations. As part of the audit, the controls over the information systems used in the ticketing process were also examined.

The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing. Audit fieldwork was conducted from September 1, 2010 to December 9, 2010.

Our audit included the Department's ticket revenue collected during the period of July 1, 2009 through June 30, 2010. Total revenue from ticket sales received by the Department for the year ended June 30, 2010 was $553,660. Of this amount, $481,535 was from football events and $72,125 was from all other sports, including: basketball, soccer, volleyball, baseball, and softball.

The audit included tests of the accounting records and such other auditing procedures as we considered necessary. We reviewed University policies and procedures, and Florida statutes, observed current practices and processing techniques, interviewed responsible personnel, and tested selected transactions. Sample sizes and transactions selected for testing were determined on a judgmental basis.

The scope of the information systems work performed focused on the evaluation of software access controls and internal user account management controls associated with the online software application and its associated ticket sales site. The objective of the information systems audit included:

- The adequacy of the current process regarding the addition, modification, and removal of user access
- The appropriateness of current user access specific to privileged and other high risk access roles
- The adequacy of Segregation of Duties specific to privileged users accounts
- Determining that basic security measures have been implemented for end user workstations which access the online application.

To achieve our information systems objectives, the following methodologies were applied:

- Control Objectives for Information and related Technology (COBIT) 4.1 (User Account Management, Identity Management, Segregation of Duties, and Malicious Software Prevention, Detection, and Correction); and
- National Institute of Standards and Technology (NIST) Special Publication 800-53A Revision 1 (Access Control Policy and Procedures, Account Management, and Personnel Termination).

As part of our audit, we reviewed internal and external audit reports issued during the last three years to determine whether there were any prior recommendations related to the scope and objectives of this audit and whether management had effectively addressed prior audit concerns. No prior recommendations were noted related to Athletics Department ticket sales.

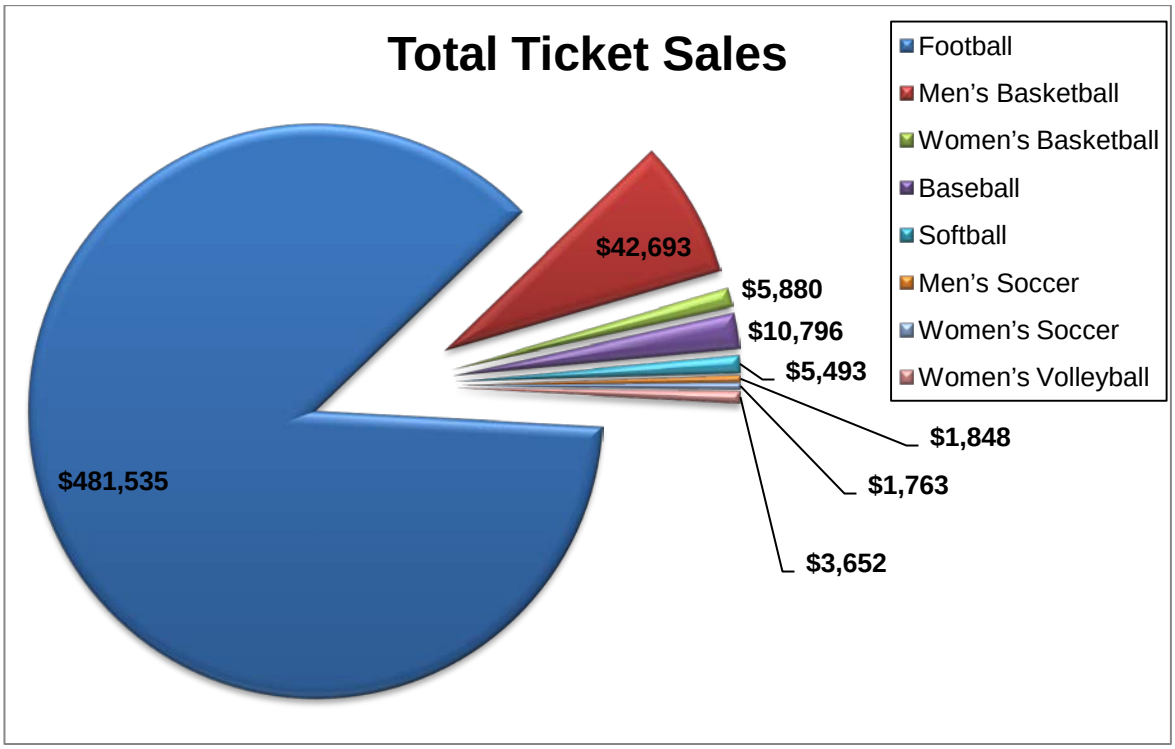
BACKGROUND

The University is a Division I, Football Bowl Subdivision participant of the NCAA and a member of the Sun Belt Conference for both men and women's sports, except for the men's soccer program which competes as an associate member in Conference USA. Men's sports consist of football, basketball, baseball, soccer, and cross country/track & field. Women's sports consist of basketball, soccer, softball, cross country/track, volleyball, swimming & diving, tennis, and golf. Only football, soccer, volleyball, basketball, baseball, and softball are revenue-generating sports. The Athletics Department's sale of athletic tickets is governed by the University Cash Control Policy and the University Departmental Cash Collection Procedures Manual.

The sale of all University sporting event tickets is performed at the stadium box office and is supervised by the Ticket Office Manager. The Ticket Office also employs one Assistant Manager, one part-time staff employee, and four student interns. Additionally, the University contracts with a vendor to provide extra cashiers and supervisors, as needed, to assist with the sale of tickets during game day. Total payments to this vendor for the 2010 season were $8,174.

Tickets are sold in one of three methods: on the phone, through the internet, or in person at the box office. Athletics has contracted with an online Ticketing Services application vendor (see Finding No. 5) to account for the sale of all tickets, regardless of the method of sale. All transactions involving the sale of tickets is logged in the online vendor's system and batch entries are later made to record the activity into the University's PantherSoft Financial System.

Revenue collected from the sale of tickets by each sport during the audit period is depicted in the following chart:



FINDINGS AND RECOMMENDATIONS

Based on our audit, we have concluded that, except for certain controls requiring additional strengthening, the Athletics Department's controls and procedures over the sale of athletic tickets are generally adequate and being adhered to. Transactions tested were, for the most part, in compliance with University policies and procedures and applicable state statutes, rules and regulations. However, our audit of the controls over the ticket sales information systems revealed security deficiencies to the user account management process. In addition, we found super user access privileges inappropriately allocated and found workstation security monitoring capabilities were not operating as expected.

Details of our findings and recommendations follow.

1. Cash and Check Deposits

University Departmental Cash Collection Procedures requires that all cash, checks, and money orders be deposited within 48 hours of collection to the University Student Financials Office. Furthermore, deposits containing cash in excess of $5,000 must have an FIU police escort to the Student Financials Office.

During our review of the selected sales reports we noted that 5 out of the 10 selected reports had a delay in deposit ranging from 3 to 25 days. It was also disclosed that police escorts were not being used for deposits of cash larger than $5,000, as required by the procedures.

Recommendation:

Athletics should:	
1.1	Ensure all deposits are taken to the Student Financials Office within two days of collection.
1.2	Ensure that an FIU police escort is used while transferring deposits containing cash in excess of $5,000.

Management Response/Action Plan:

1.1 Ticket Office staff have generally waited to accumulate several checks in the safe before depositing funds to save the time required in taking trips to the Cashier's Office every 2 days. Management will increase the frequency of deposits going forward where deposits will be made within 2 business days as reasonably possible.

Implementation Date: Immediately

1.2 Management will request a police escort for cash deposits in excess of $5,000.

Implementation Date: Immediately

2. Employee Background Checks

University Policy No. 1710.257 requires the performance of criminal history checks on all newly hired employees. The policy also requires more in-depth criminal history checks including fingerprinting, through the Florida Department of Law Enforcement for new employees (or employees recently promoted) in sensitive positions. Included in this category of employees are individuals handling cash or managing cash transactions.

Upon review of employment files for all Ticket Office personnel managing cash transactions, none had been fingerprinted as required by the policy above. It was also noted that three Ticket Office student interns were managing cash transactions although they were not University employees, and thus, not checked for possible criminal history.

Recommendation:

Athletics should:	
2.1	Work with Human Resources to ensure that criminal background checks including fingerprinting are conducted for all applicable positions.
2.2	Ensure that only employees with the proper background check manage cash transactions.

Management Response/Action Plan:

2.1 Management will request criminal background checks including fingerprinting for all applicable positions.

Implementation Date: Immediately

2.2 Management will ensure that only employees with proper background checks will manage cash.

Implementation Date: March 2011

3. Segregation of Duties

Our review of 25 ticket stubs collected on game day disclosed that one ticket used was previously voided by University personnel. The Ticket Office Manager indicated that this voided ticket seat number was accidently voided and was actually valid. The final count of tickets sold and revenue received was proper but the voided ticket was used to enter the game.

During our test, we observed that Ticket Office personnel have the ability to sell tickets, collect payments, and void their own transactions. Allowing employees the authority to void their own sale transactions, without a supervisor's review, creates an internal control weakness.

Recommendation:

Athletics should:	
3.1	Ensure that there is adequate separation of incompatible duties, or alternatively, design mitigating controls, which would include a review of executed voids.

Management Response/Action Plan:

3.1 Segregation of duties is particularly difficult due to the limited number of staff working in the Ticket Office. Management will establish mitigating controls including; the periodic review of voided transaction reports to include notes on the reason for the voids which will be signed by the Ticket Office Manager and provided to the Associate AD Finance for review on a quarterly basis.

Implementation Date: March 2011

4. Reconciliation of Ticket Sales Reports

The reconciliation between the PantherSoft postings and the online ticket vendor's sales reports needs to be more thorough. In October 2009, part of a credit card transaction was omitted from the online vendor's records. This difference remained unnoticed by Athletics Department personnel for five months. Until the correction, the online vendor's and PantherSoft records did not balance.

In addition, upon our review of 10 daily sales reports, we observed that the review process was insufficient. Ticket Office reconciliation forms were not signed to document who the preparer was or as evidence that reports were being reviewed. This lack of review may have led to the difference in the reconciliation noted above not being corrected in a timely manner.

Recommendation:

Athletics should:	
4.1	Perform periodic reconciliations between the PantherSoft postings and the online vendor's sales reports and ensure all differences are identified and corrected.
4.2	Review Ticket Office reconciliation forms for accuracy and require signatures to document the preparer and reviewer's actions.

Management Response/Action Plan:

4.1 The difference between the daily sales report from the point of sales system and the credit card processor of $75 was generated by a system anomaly recognized by the vendor. This was caught as part of the daily review, but was not followed up in a timely manner. Management agrees with this recommendation and will monitor both the transaction data detail and perform periodic reconciliations with the online vendor's point of sales reports.

Implementation Date: Immediately

4.2 Ticket Office reconciliation forms will be reviewed. Management will require signatures to document the preparer and reviewer's actions.

Implementation Date: Immediately

5. Contracting Process

According to the University Purchasing Department Procedures Manual, University personnel are not allowed to sign contractual agreements of any type with vendors. All contracts should be forwarded to Purchasing Services with a "Contract In-Take Form," and if required, the contract would then be forwarded to the General Counsel's Office.

The Athletics Department entered into an undated agreement with Complete Ticket Solutions to provide ticket operations assistance during the 2010 football season at a cost of "approximately $7,750." The agreement was not submitted to Purchasing Services for review and was signed by the Ticket Office Manager who is not authorized to sign contractual agreements. In addition, the agreement was designated for assistance during football games but we noted the company was contracted for other sporting events as well, such as basketball, which were not included in the agreement.

Recommendation:

Athletics should:	
5.1	In the future, forward all contracts to the Purchasing Services Department and not allow unauthorized personnel to sign agreements with vendors.

Management Response/Action Plan:

5.1 The Ticket Office Manager reviewed the contract with several Athletics Department administrators including the Athletics Director before signing. Management does recognize that only the Athletics Director has signature authority and will be the sole signatory on contracts going forward. Management is working with the General Counsel's office to modify procedures in order to streamline the process while maintaining compliance.

Implementation Date: Immediately

Auditors' Comment: The Purchasing Department has been delegated certain duties pursuant to FIU Regulation §2201, *Purchasing*. The purpose of this regulation is to ensure that procedures, and practices used in acquiring commodities and services are appropriate. The Office of Internal Audit wishes to reiterate that the Athletics Department should comply with current University procedures and practices.

6. Ticket Sales Website Discrepancies

During our review of the football ticket sales website, we noted some discrepancies. We found the coloring of the seating chart sections did not agree with the colors of the various price levels, thus, making it difficult to identify the correct pricing of a section. Also two sections were listed at two different price levels and two other sections were not listed at all. However, we did not identify any issues with improperly priced tickets being issued.

Recommendation:

Athletics should:	
6.1	Ensure that the football ticket website provides accurate information to customers selecting their tickets.

Management Response/Action Plan:

6.1 Management agrees that further refinement of the published ticket seating diagram including separation of colors and price levels would improve clarity for the customer.

Implementation Date: May 2011

7. Access Control Policies

According to NIST[1] AC-1.1 and good business practice, access control policies should be developed and formally documented. The access control policy should address purpose, scope, roles and responsibilities, legal and regulatory guidelines. There should be a defined frequency for reviewing and updating access control policies. Access Control policies should be reviewed and updated in accordance within the University-defined frequency.

During our review, we noted that there are no formally documented access control policies available.

Recommendation:

Athletics should:	
7.1	Develop and document a formal access control policy. Formal policies should include, purpose, scope, roles and responsibilities, and adhere to legal and regulatory guidelines.
7.2	Review and update the access control policies on a periodic basis.

Management Response/Action Plan:

7.1 A new point of sale software used for ticket sales was implemented in the summer of 2009 which required considerable setup and training. Now that the learning curve has flattened, management will formalize and document control policy, roles, and responsibilities. The written control policies will be within the legal and regulatory guidelines.

Implementation Date: August 2011

7.2 Upon completion of 7.1, management will review and update policies periodically.

Implementation Date: August 2011

[1] National Institute of Standards and Technology Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems and Organizations

8. Access Control Procedures

According to NIST AC-2.1 and good business practice, user account management should include establishing, activating, modifying, disabling, and removing of user accounts. User account managers should be notified when temporary accounts are no longer required and when information system users are terminated, transferred, or application usage or need to know changes. User account management should deactivate temporary, terminated, and transferred accounts that are no longer required. Access control management should grant access to the application based on a valid access authorization and intended application usage.

We found the on-boarding and off-boarding process to be informal and ad hoc. We also found that there are not adequate procedures in place to ensure that access capabilities were timely revoked for individuals who had terminated employment. In tests of 44 active user accounts, we identified 12 formerly terminated user accounts (10 former FIU employees, and 2 former apparel providers) were still active. There was also 1 user account which could not be accounted for.

Recommendation:

Athletics should:	
8.1	Ensure to deactivate the 12 formerly terminated user accounts and the 1 unaccounted for account.

Management Response/Action Plan:

8.1 Management agrees to deactivate the 12 formerly terminated user accounts and the 1 unaccounted for account.

Implementation Date: Immediately

9. Information System Account Management Functions

According to NIST (AC-2(1).1, AC-2(2).1, AC-2(3).1) and good business practice, user account management should automate mechanisms to support information system account management functions. User account management should have a defined time period for each type of account after which the information system terminates temporary and emergency accounts. The information system should automatically terminate or disable temporary, emergency, and inactive accounts after a defined time period.

During our testing, we noted that there are no automated user account deactivation mechanisms in place for either terminated or temporary users.

Recommendation:

Athletics should:	
9.1	Implement an automated user account deactivation process for terminated and temporary user accounts, or alternatively, design other processes which will ensure the deactivation of terminated and temporary user accounts.

Management Response/Action Plan:

9.1 Management will explore the possibility and cost associated with this software modification with the vendor. Depending on criteria established, vendor feedback, and cost, this recommendation may not make economic sense. This initiative will be lead by the Assistant AD for Media Relations and will begin at the conclusion of the 2011 Men's Basketball season.

Implementation Date: April 2011

10. User Account Audit Trail

According to NIST AC-2(4).1 and good business practice, the information system should automatically audit account creation, modification, disabling and termination actions. The information system should notify, as required, appropriate individuals.

We found that the application does not maintain an audit trail for user accounts creation, modification, disabling, and termination actions.

Recommendation:

Athletics should:	
10.1	Consult with the software developer to ensure that the application maintains a user account audit trail. The user account audit trail should retain account creation date, account disable date, the user profile and date modified, last date user logged in, user previous access roles and permissions. An automated trigger mechanism should be used to notify the system administrators group when privileged and or sensitive access has been granted.

Management Response/Action Plan:

10.1 Management will explore the possibility and cost associated with this software modification with the vendor. Depending on criteria established, vendor feedback, and cost, this recommendation may not make economic sense. This initiative will be lead by the Assistant AD for Media Relations and will begin at the conclusion of the 2011 Men's Basketball season.

Implementation Date: April 2011

11. Identity Management

According to NIST AC-2.1 and good business practice, information system accounts should include identifying the account type (i.e. individual, group, system, application, custom, privileged, guest/anonymous, and temporary); establishing conditions for group membership; identifying authorized users of the information system and specifying access privileges; require appropriate approvals for request to established accounts; and specifically authorizing and monitoring the use of privileged, guest/anonymous and temporary accounts.

We noted that Identity Management is entirely managed internally within the Athletics Department. The vendor application has five (5) role-based user access levels: Full Access (Donor); Full Ticket Office Access; Read Only (Donor); Report Only (Ticket Office); and Ticket Office Game Day Sales. We found that 66% (2 of 3) user accounts in the Ticket Sales and Operations Department have a role-based user access level. There are no formal processes to assign group membership or obtain access request approval. In addition, high risk accounts including guest/anonymous, temporary, and privileged accounts are not monitored.

The use of generic user accounts diminishes the effectiveness of user account management. In our testing, we identified 11 generic user accounts, including 1 test user account, 1 third-party user account, 4 third-party ticket sales, and 5 third-party generic (Site Administration, Internet Agent, Payment Plan Agent, Ticket Donations, and Internet Sales) accounts.

Recommendation:

Athletics should:	
11.1	Implement a formal process when assigning users to role-based access levels.
11.2	Ensure that FIU employees not use generic user accounts.
11.3	Ensure that temporary generic user accounts are only enabled when in use by non-FIU employees.

Management Response/Action Plan

11.1 As stated in 7.1 a new point of sale software used for ticket sales was implemented in the summer of 2009 which required considerable setup and training. Now that the learning curve has flattened, management will formalize and document control policy, roles, and responsibilities. The new policy document will include a formal process for assigning users to role-based access levels.

Implementation Date: August 2011

11.2 Management will ensure that generic user accounts will not be used by FIU employees. The Ticket Office will create accounts specific to Ticket Office employees.

Implementation Date: Immediately

11.3 Management will ensure that generic accounts will only be used by non-FIU employees.

Implementation Date: Immediately

12. Least Privileged Account Access

According to NIST (AC-6.1, AC-6(4).1, AC-6(5).1, AC-6(6)) and good business practice, the concept of least privileged should be employed, allowing only authorized access for users (and process acting on behalf of users) which is necessary to accomplish assigned tasks in accordance with organizational missions and business functions. The information system should provide separate access selections to enable finer-grained allocation of user privileges. Super user accounts authorization should be limited on the information system to designated system administration personnel. Privileged access to the information system by non-University users should be prohibited.

We noted excessive super user access for the Assistant AD in the Ticket Sales and Operations Department. Additionally, we noted excessive super user access for 100% (6 of 6 users) of the Media Relations Department and one Assistant Development Director.

During our fieldwork, we noted that access provisioning is provided by the online vendor.

Recommendation:

Athletics should:	
12.1	The number of super user access accounts should be limited to designated system administration personnel.
12.2	Be responsible for all user access provisioning.

Management Response/Action Plan:

12.1 Management will review employee functions and user access levels in order to determine who needs super user access. Once a complete understanding of the limitations is determined, super user access will be limited.

Implementation Date: March 2011

12.2 Management would like super user access assigned to the Assistant Athletic Director of Ticket Sales and Operations, and the Assistant Athletic Director of Media Relations, and does not consider the current access for these users to be excessive. Management does however agree that access should be and will be limited for other users based on recommendation 12.1. Super user access is imperative for essential job functions.

Implementation Date: March 2011

13. Workstation Security

According to NIST SI-3.1 and good business practice, workstation security should include the ability to detect and eradicate malicious code including files transported by electronic mail, electronic mail attachments, web access, removable media or other common means. Workstations should update its malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policies. Malicious code protection mechanisms should define the frequency of periodic scans of the information. Defined actions should be taken (block, quarantine, and or alert administration) in response to malicious code detection. Malicious code protection mechanisms should be defined to perform real-time scans from external sources as the files are downloaded, opened, or executed in accordance with security policy. The information system should prevent non-privileged users from circumventing malicious code protection capabilities.

The University deploys McAfee's On-Access Scanner (OAS) to mitigate the risk of viruses. The purpose of OAS is to scan files and folders as they are being accessed and either block or quarantine viruses before they are able to affect the information systems. During our testing, we found OAS disabled on one workstation. A disabled OAS increases the risk of obtaining viruses thereby reducing the effectiveness of information systems security efforts.

Recommendation:

Athletics should:	
13.1	Have UTS enable OAS on the identified workstation.
13.2	Have UTS perform root cause analysis on the identified workstation. As the cause may affect additional workstations within the University, the results from the root cause analysis should be documented and distributed to appropriate parties to ensure all workstations are uniform.

Management Response/Action Plan:

13.1 FIU Athletics has contacted FIU UTS to address this recommendation. This is their response: The FIU IT Security Office will determine the cause for the OAS being set to the "disable" mode and take corrective action to insure it is enabled on all workstations and remains in that state.

Implementation Date: February 2011

13.2 Please see response to 13.1

Implementation Date: February 2011

14. Penetration Testing

According to NIST sp800-53A Rev.1 Appendix E and good business practice, controlled penetration testing should be added to the tools and techniques used to assess the security controls in information systems. Penetration testing is a specific type of assessment in which assessors simulate the actions of a given class of attacks. Penetration testing is conducted as a controlled attempt to breach the security controls employed within the system. Penetration testing should not be viewed as a means to verify the security of an information system, but rather as a means to: (1) enhance the understanding of the system; (2) uncover weaknesses or deficiencies in the system; and (3) indicate the level of effort required on the part of adversaries to breach the system safeguards.

We noted that the University has not performed or reviewed any third-party penetration testing of the online ticketing sales website. We performed limited high-level testing on the online ticketing sales website. We noted weak password parameters and lack of account lock-out after a specific number of unsuccessful tries.

Recommendation:

Athletics should:	
14.1	Work with the Information Technology Security Office to coordinate with the software application vendor a documented controlled penetration test on an annual basis to ensure the online ticket sales website's security controls are adequately protecting the confidentiality, integrity, and availability of its information resources. The controlled penetration test report results should include proof of mission risks; indicate the level of effort an adversary would need to expend in order to cause harm to the University; define threat sources; document all activities performed during the test, including all exploited vulnerabilities and how the vulnerabilities were combined into attacks; ensure the effectiveness of existing security controls, such as firewalls, intrusion detection and prevention systems; and provide actionable results with information about possible remediation measures for the successful attacks performed.
14.2	Coordinate with the software application vendor to strengthen password and account lock-out parameters to mitigate the risk of unauthorized access and of a "brute force" attack.

Management Response/Action Plan:

14.1 FIU Athletics has contacted FIU UTS to address this recommendation. Please see their response: The FIU IT Security Office will compose the Annual RFQ for the penetration test to be performed on the recommended environment. The FIU IT Security Office will also manage the vendor and work with Athletics on remediation of issues identified.

Implementation Date: March 2011

14.2 Please see response to 14.1

Implementation Date: March 2011