DEPARTMENT OF INTERCOLLEGIATE ATHLETICS

INFORMATION TECHNOLOGY

AUDIT REPORT #17-4003

Audit & Advisory Services

August 2017

DEPARTMENT OF INTERCOLLEGIATE ATHLETICS

INFORMATION TECHNOLOGY

 AUDIT REPORT #17-4003

Background

In accordance with the Campus fiscal year 2016-17 audit plan, Audit & Advisory Services (A&AS) conducted an audit of information technology general controls within the Department of Intercollegiate Athletics (UCLA Athletics).

The UCLA Athletics Information Technology (IT) department is dedicated to providing technological support to administrative staff and coaches of UCLA Athletics. There are approximately 2,818 employees in UCLA Athletics:

* Career – 157
* Contract – 128
* Limited – 1,761
* Students – 772

The IT department is committed to developing, adopting, and maintaining appropriate policies, standards, and procedures to meet and manage the UCLA Athletics administrative and sports operation’s needs. The IT department performs purchasing and maintenance of computer equipment, phones, and technological devices. The IT department is responsible for evaluating, installing, testing, configuring, maintaining, and backing up application servers. They implement data security and network component physical security measures, perform backup and file recovery procedures, provide remote network administration capabilities, and site software license and equipment inventory controls over installed network components. Software training, general hardware and software troubleshooting, and other technical support is also provided to departmental employees.

The IT department manages:

* Laptops: 282
* Mobile Devices: 273
* Desktops: 81
* Applications: 12
* Third-party vendor system integration: 8
* Portals and Web Sites: 5
* BruinClock Applications: 5
* SharePoint Libraries/Sites: 4
* Mobile Apps: 3

The IT department consists of four career employees and one student worker. The Assistant Athletics Director of IT oversees the operation, and reports to the Senior Associate Athletic Director/Chief Financial Officer.

Purpose and Scope

The purpose of the review was to ensure that the organizational structure and controls, and the related systems and procedures surrounding IT general controls within the UCLA Athletics IT department are conducive to accomplishing the University’s business objectives. Where applicable, compliance with University and departmental policies and procedures was also evaluated.

The scope of the review focused on the following areas:

* Identity and Access Management
* System Controls
* Physical Security and Environmental Controls
* Disaster Recovery and Business Continuity

The review was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and included tests and other procedures considered necessary in achieving the audit purpose. Interviews were conducted with management and staff, and various other administrative documents related to IT controls were examined.

Summary Opinion

Based on the results of the work performed within the scope of the audit, the UCLA Athletics IT department has established adequate internal controls and business practices to help ensure that the University’s business objectives are met. The audit identified the following areas where internal controls could be further strengthened:

*Identity and Access Management*

* Management should ensure that separated and transferred employee access is disabled in a timely manner to help deter unauthorized access to systems and applications.
* To maintain accountability, generic user accounts should not be used. Each user should have their own Active Directory account.
* The Active Directory should include the employee’s official name per the Personnel Payroll System (PPS) and their employee University Identification (UID) number to enhance the data integrity of the user listing.
* The Active Directory should be reviewed to ensure that all users have their correct UID listed. The correct UID listed for each user increases the data integrity of the Active Directory listing.
* Management should review the Active Directory listing and ensure that all users are active employees of the UCLA Athletics department and verify that their access is appropriate.

*System Controls*

* Management should establish technical security mechanisms such as computer session timeouts to minimize unauthorized access to restricted or essential services or devices that are left unattended for an extended period of time.
* The IT department should create separate administrative accounts and the user activity of the administrative accounts should be logged and periodically monitored by an independent and knowledgeable individual.
* Password controls should be strengthened.
* Management should establish formal change management procedures.
* Management should create documentation standards for the systems and applications that are developed and maintained by the UCLA Athletics IT department.

*Physical Security and Environmental Controls*

* Management should increase the physical controls over the server rooms located in the UCLA Athletics IT office and Acosta Training Center by installing entry alarms, and consider installing a security camera to monitor the server rooms. Also, management should review the environmental controls over the server room in the Acosta Training Center to ensure that potential hazards do not exist, and install moisture alarms in both server rooms.

*Disaster Recovery and Business Continuity*

* Management should update the current disaster recovery and business continuity plan. Also, a business impact analysis should be conducted to reflect current processes and to aid in disaster recovery and business continuity planning.

In addition, UCLA Athletics IT staffing requirements should be evaluated on a regular basis or upon major changes to the business, operational, or IT environments to ensure that the IT function has sufficient resources to adequately and appropriately support the business goals and objectives of the department. Based on the above observations on how internal controls could be strengthened, it appears the current staffing may not be enough resources for the size of the IT function they support.

The audit results and corresponding recommendations are detailed in the following sections of the audit report.Audit Results and Recommendations

Identity and Access Management

Active Directory (AD) is used by the IT department to grant users access to their computers and to certain systems. When a person needs to be added to AD, the IT department receives a notice from Athletics Human Resources (HR) requesting that the employee be added. Likewise, when a user transfers or separates, HR sends an email to the IT department notifying them that the user needs to be removed from AD. As of June 23, 2017, AD consists of 383 users; 378 are unique employee accounts and five are generic accounts. Audit test work indicated the following:

1. Separated Employees

Thirty-three users are previous employees of UCLA Athletics and have separated from UCLA. The separation dates of the users ranged from July 31, 1995 to June 4, 2017. See the table below for a summary of users by separation year:

|  |  |
| --- | --- |
| **Separation Year** | **# of Users** |
| 2017 | 8 |
| 2016 | 11 |
| 2015 | 7 |
| 2014 | 4 |
| 2013 | 2 |
| 1995 | 1 |
| **Total** | **33** |

Recommendation: Management should ensure that separated and transferred employee access is disabled in a timely manner to help deter unauthorized access to systems and applications.

Response: DIA has reviewed the recommendation and has addressed the outstanding employees noted. The department’s IT and HR staff will collaborate to address staff changes in real time as well as conduct periodic audits of the overall list to ensure accuracy of active staff. For example, the DIA HR staff includes the IT staff when new staff is on-boarded (as well as off-boarded) to ensure accuracy.

1. Generic Accounts

Test work indicated there are five generic user accounts. Review of the display names for the generic accounts indicated the following:

* *Team Doctor* – Used by doctors in Athletics Training.
* *Sports Medicine* – Used by student trainers in Sports Medicine.
* *BVC (Bruin Varsity Club) Intern* – Used by student interns.
* *Test Font* – Used to test user control over installing fonts.
* *Security Desk* - An account that appeared generic by having the first name "Security Guard" and last name “Morgan Center,” is actually used by the current security guard. The login includes part of their name. To prevent the account from appearing generic, the name listed for the user should be the employee's name.

After discussions with A&AS, IT management disabled the *Test Font* and *BVC Intern* accounts.

Recommendation: To maintain accountability, generic accounts should not be used. Each user should have their own AD account.

Response: DIA has begun the process of removing generic accounts as noted above and will phase them out over the next few months, transitioning those that need access to their own account.

1. Missing University Identification (UID) Numbers

The UID number was missing from 195 AD accounts. The employee’s UID is currently entered in the "P.O. Box” field by Athletics HR. Discussions with IT management indicated that it has not been a normal business practice to update the field with an employee’s UID if it is missing.

Recommendation: The AD should include the employee’s official name per PPS and their employee UID number to enhance the data integrity of the user listing.  The UID is a unique identifier and using the employee’s official name adds uniformity. Additionally, by including the UID in all AD accounts, data analytics can be performed using the UID to ensure that all users are current employees of UCLA Athletics.

Response: DIA staff (HR and IT staffs) are working closely to input needed ID numbers and ensure that they are provided when staff are hired and within the on-boarding email when possible. If not possible, then at a later date as the information is generated by campus. Periodically HR and IT staff will review to ensure accuracy.

1. Duplicate University Identification (UID) Numbers

Nineteen users had a UID number listed in their profile that belonged to another UCLA Athletics employee:

* In eleven instances, active employees had a UID listed that belonged to another active Athletics employee.
* In seven instances, active employees had a UID listed that belonged to an Athletics employee that was separated from the University.
* In one instance, a separated employee had a UID listed that belonged to an Athletics employee that had already separated from the University.

Recommendation: The AD should be reviewed to ensure that all users have their correct UID number listed. Having the correct UID listed increases the data integrity of the AD listing.

Response: Similarly, the responsible DIA staff (HR and IT staffs) are working closely to input accurate ID numbers when staff are hired within the on-boarding email when possible. If not possible, then at a later date as the information is generated by campus. Periodically HR and IT staff will review to ensure accuracy.

1. Users without University Identification (UID) Numbers

Through review of the PPS Employee Database (EDB), A&AS was unable to find the UID number or the identity of 26 of the users.

Recommendation: Management should review the user accounts of the 26 people who were not found in PPS EDB and determine whether they are active employees of UCLA Athletics and verify that their access is appropriate.

Response: DIA IT and HR departments have addressed the 26 incorrect names and will work closely to verify these at the beginning.

System Controls

A review of system controls included those related to session protection, administrative access, password security, patch management, change management, and systems development. The following were noted:

1. Session Protection – Timeouts on Computers

The IT department has responsibility for purchasing, setting up, and maintaining all the computers for Athletics.  However, the IT department has not established session timeouts on computers that function is left up to the user.  According to UC Business and Finance Bulletin IS-3, “Electronic Information Security” (IS-3), Session Protection [III.C.2.b.ii] “Devices that access restricted and/or essential services that are left unattended for an extended period of time shall employ measures, such as session timeout or lockout mechanisms, that require re-authentication before users return to interactive use.  Devices that host confidential or critical information may be subject to additional requirements."

Recommendation: To comply with IS-3, management should establish technical security mechanisms such as computer session timeouts to minimize unauthorized access to restricted or essential services or devices that are left unattended for an extended period of time.

Response: DIA IT staff is adjusting the Windows group policy to address the recommendation in accordance with IS-3 policy and distribute to all DIA staff. The entire DIA staff will be notified at the first all staff meeting of the year, if not individually beforehand. Follow-ups will occur by department throughout the year to ensure compliance.

1. Administrative Access

In early March 2017, a decision was made to remove administrative rights from the IT staff's user accounts and instead use an “admin user account” that would be shared by the staff.  IT staff would logon to the account when they need to use it.  The administrative account is appropriately limited to the IT staff who need it based on their job function. The admin user account is used for administrative work on the servers, setting up new computers, and for general troubleshooting. The following issues were noted:

* The admin account is a shared account.
* An audit trail is not maintained on who used the account, it is only tracked within the Windows event log.
* The activity of the administrative account is not logged.

According to guidance on privileged users stated in IS-3, Security Plan, [III.C.2.b.iii]:

* Personnel who require privileged accounts should also have non-privileged accounts to use when not performing system administration tasks and should be instructed not to use their privileged accounts for non-authorized purposes.
* Activities performed using a privileged account should be logged, where feasible, and the logs should be reviewed on a regular basis by an independent and knowledgeable person.
* Use of privileged accounts should be monitored periodically to ensure they are being used for authorized purposes.

Recommendation: UCLA Athletics IT should create separate administrative accounts and the user activity of the administrative accounts should be logged and periodically monitored by an independent and knowledgeable individual.

Response: DIA IT staff has executed as noted and created separate accounts for those needs.

1. Password Controls

Discussions with IT department staff indicated the following:

* The complexity requirement for passwords is that they must be six characters in length.
* Default passwords are changed immediately.
* Users are encouraged to change passwords. Passwords expire every 42 days.
* Password history is maintained to prevent reuse of the last password.
* Passwords are properly masked on the system.

According to UCLA Policy 401, “Minimum Security Standards for Network Devices,” all passwords employed to authorize access to campus electronic communications systems or services must meet the following minimum password complexity standards. The password must:

* Contain eight characters or more.
* Contain characters from at least two of the following three character classes:

Letters (a-z, A-Z)

Numbers (0-9)

Special characters including a space (:!@#$%^&\*()\_+|~-=\`{}[]:";'<>?,./)

Recommendation: To comply with UCLA Policy 401, password controls should be strengthened.

Response: As noted above DIA IT staff will roll out a new policy to the entire DIA staff in the near term once all staff are back at the beginning of the school year and then follow up periodically to ensure compliance.

1. Patch Management

The IT department has established appropriate procedures that ensure the timely update of security patches. Automatic Updates is on all Windows computers and left at its default settings which is scheduled for everyday at 3 a.m. Patches are reviewed to ensure they do not interfere with servers or applications.

There were no significant control weaknesses identified in this area.

1. Antivirus

UCLA Athletics IT uses the Sophos Antivirus software. Using patented InterCheck technology, Sophos's "on-access" scanner provides constant real-time protection with minimal system overhead. Sophos shields networked devices from malicious software, such as viruses, spyware, and other types of malware.  All devices are purchased through the IT department who installs Sophos as part of the setup process. Updates are installed daily through the auto-updater. Additionally, a firewall is in place to allow only authorized traffic to cross the network.

There were no significant control weaknesses identified in this area.

1. Change Management Policy

Athletics IT does not have a formal change management policy. Change requests are emailed to the IT department, the request is reviewed, tested, and then put into production. For newer projects, GitHub is used. GitHub is a development platform that is used for newer projects and it provides a repository of the code used, source documentation, and version control.

According to IS-3, Change Management [III.C.2.d], “Maintaining system integrity requires that all changes to a system are conducted according to a planned and supervised change management process.” Change management procedures should include:

* Monitoring and logging of all changes
* Steps to detect unauthorized changes
* Confirmation of testing
* Authorization for moving application programs to production
* Tracking movement of hardware and other infrastructure components
* Periodic review of logs
* Back out plans
* User training

Recommendation: Management should establish a formal change management policy.

Response: DIA IT will review its policy to address concerns in a timely manner for the department staff size and needs. All changes have been made in writing and will continue to be done in a similar manner for any changes made to policy if needed.

1. Systems Development Standards

The Athletics IT department plans, designs, develops, implements, maintains, and documents business desktop and web applications; establishes timelines for the applications to be developed as well as prototypes; performs integration testing; releases applications in beta version, and once tested, puts the applications into production. The IT department also schedules maintenance for applications.

Test work indicated the development and maintenance of UCLA Athletics information systems do not conform to the specifications of UC Business and Finance Bulletin IS-10, “Systems Development Standards” (IS-10).  System definition documentation standards provide information on the functional office that will use the new system, system architecture, database design, sources of data, privacy consideration, and backup and recovery.

IS-10 [B.14], recommends the following written documentation:

* Operations Manual: Contains information required for the production control group to run batch portions of the system, if any.
* Systems Manual: For use by those responsible for on-going maintenance of the system.
* User Documentation: Contains instructions for the functional office(s) on how to use the system, and may be combined, if appropriate, with the functional office’s internal procedures manuals.

Recommendation: Management should create documentation standards for the systems and applications that are developed and maintained by the UCLA Athletics IT department.

Response: DIA IT staff is working to develop standardized code management system through Github to address recommendation. Operation policies and procedures are maintained, and each end user has instructions on how to use necessary documents (DIA Financial Portal has information maintained by owner/user – Business and Finance staff) and can incorporate those into larger manual’s as needed.

Physical Security and Environmental Controls

A&AS reviewed physical security policies for the server environment to determine if physical access controls are sufficient. IT personnel were interviewed regarding the environmental and physical access controls relating to the two server rooms. In addition, the two server rooms were physically inspected on May 19, 2017.

The servers are housed at two locations within UCLA Athletics. The locations (IT department office and Acosta Training Center) include uninterruptible power supply (UPS) protection, resilient network connectivity, servers that are on raised racks, a waterless fire suppression system, automatic backup generators, and heating, ventilation, and air conditioning (HVAC). They are equipped with temperature and smoke monitors and alarms. Physical access to the server rooms is adequately controlled through keys that are stamped “Do Not Duplicate,” and the rooms are restricted to only authorized personnel.

The following issues were noted:

* The server rooms are not equipped with entry alarms or video surveillance.
* The Acosta Training Center server room has a water supply pipe that is installed near the servers, which is a potential hazard.
* The server rooms do not have moisture alarms.

Recommendation: Management should increase the physical controls over the server rooms located in the IT office and Acosta Training Center by installing entry alarms, and consider installing a security camera to monitor the server rooms. Also, management should review the environmental controls over the server room in the Acosta Training Center to ensure that potential hazards do not exist and also install moisture alarms in both server rooms.

Response: DIA IT staff and space is limited within facilities and will explore moisture-tracking devices in appropriate areas. In addition, many venues already have cameras monitoring entry/exit from facilities to ensure knowledge of individuals.

Disaster Recovery and Business Continuity

Disaster recovery and business continuity were evaluated based on discussions with IT personnel and review of the Athletics Disaster Recovery Runbook.

Based on audit review, UCLA Athletics does have a disaster recovery and business continuity plan. The disaster recovery and business continuity plan was last tested June 2016, but was not formally documented. The following were noted:

* Although all four members of the IT department are familiar with the plan, review of the Disaster Recovery Runbook showed that members of the recovery team and other relevant staff are not listed in the plan, nor does it describe their responsibilities and roles.
* The Disaster Recovery Runbook does not provide identification and prioritization of the activities that are essential to continue functioning.
* The plan was not based upon a business impact analysis that considers the impact of the loss of essential functions.
* The plan does not identify the resources that will likely be needed for recovery and the location of their availability.

According to UC Business and Finance Bulletin IS-12, “Continuity Planning and Disaster Recovery” (IS-12), disaster recovery plans should be tested on a periodic basis and plans should be updated to reflect changing environments, processes, technology, or other impacts as appropriate.

A disaster recovery and business continuity plan helps outline the actions needed for short-term and long-term recovery of resources and mission-critical functions. Continuous updates to the disaster recovery and business continuity plan are needed to ensure that the IT department addresses emerging and changing risks. Also, plans should be tested periodically to ensure that they are effective in reducing risk and minimizing disruption to UCLA Athletics activity in the event of an emergency or disaster.

Recommendation: Management should update the current disaster recovery and business continuity plan. Also, a business impact analysis should be conducted to reflect current processes and to aid in disaster recovery and business continuity planning. The disaster recovery and business continuity plan should be tested periodically and the test should be documented.

Response: DIA IT will review the current program which has been successful in the past and collaborate with campus IT to review best practices and address as needed moving forward.

170718-2

REP