PROJECT SUMMARY

Overview

Information technology (IT) processes and controls within Computing and Information Services (CIS) at Texas A&M University provide reasonable assurance that resources are used in compliance with laws, policies, regulations, and rules. The Open Access Lab unit maintained efficient and effective processes for deployment and imaging of student lab workstations and monitoring of lab utilization through real time statistics. Opportunities for improvement were identified in the areas of logical security and operation of the centralized help desk.

CIS is responsible for providing computing resources, services, and support to Texas A&M University, as well as other members of the A&M System. CIS operates as a university service center with a budget of approximately $30 million and 206 full-time employees.

OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

1. Logical Security

Observation

Logical security should be improved to better protect IT resources.

Improvements in logical security controls are needed to increase the university’s overall IT security. Limited weak logical security practices were noted in the areas of password management, software patch updates, and pre-logon banner use. Logical security was reviewed for systems

Logical Security

Logical security consists of software safeguards for an entity’s information systems including user IDs, passwords, anti-virus protection, operating system patch updates, encryption, and workstation security mechanisms. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation.
1. Logical Security
(cont.)

administered by three CIS units: Information Technology Solutions and Support (ITSS); Open Access Labs (OAL); and Supercomputing. These systems included UNIX/Linux and Windows operating systems and databases.

For the ITSS and OAL Linux systems tested, at least three weak default password settings were in place for local accounts. While users are assigned to groups through which password settings are normally assigned, university-required password settings should also be in place for any accounts set up locally on the machines. This also applies to the supercomputing environment. Password controls also need to be strengthened on the other systems tested including an ITSS Oracle database default profile, four ITSS Windows servers, and the OAL domains.

Patch management deficiencies were noted on various systems including some systems that were running unsupported versions. Three of the 12 (25%) ITSS Windows servers selected had a patching gap that exceeded 90 days, two of which were due to a changeover in personnel. Two of the three OAL Linux servers tested were running older, unsupported versions of the operating system. Both are in the process of being replaced with a different operating platform. One of the two OAL databases tested was found to be unsupported due to a missing service pack. Additionally, 22 of 69 (32%) Apple OS X systems tested on the OAL domain were not using the latest updated version. Management has delayed updating to the latest version due to compatibility issues with currently used software.

Texas Administrative Code (TAC) 202.75 compliant pre-logon banners were not found in place for three of the four ITSS Linux servers, all three OAL Linux servers, and the supercomputing systems.

TAC 202.70, Security Standards Policy, states that information resources are strategic and vital assets that must be available and protected commensurate with the asset's value. While the university has extensive rules and procedures in place, these were not always followed in the instances noted above. Failure to follow strong logical security practices can lead to confidential files or systems being compromised and possible disruption of critical services.

Recommendation

Implement password controls that, at a minimum, comply with university standard administrative procedures and guidelines.
1. Logical Security
   (cont.)

   Periodically review systems and accounts for compliance with password standards and guidelines.

   Patch servers, workstations and databases to the current versions and implement continuous patch management and monitoring processes.

   Implement a pre-logon banner in compliance with TAC 202.75 for all systems and include this requirement in server hardening checklists.

Management’s Response

OAL has implemented or is in the process of implementing the following:

- Password controls now meet or exceed university policy. To assist with future enforcement, a Windows password policy will be implemented at the domain level for greater control. For Linux installations, a checklist will be used that includes changing password policies. Systems will be periodically reviewed for compliance.

- System patches are current. The Apple OS is not the most current version due to compatibility issues with required software. We continue to work with the vendor to determine a solution. We anticipate having this resolved by September 2013. For continuous patch management, all the OAL servers are now under the same team that checks for updates and patches to software on a regular basis with various corresponding tools and websites. For Linux, this will include reviews as part of the scheduled monthly updates process. Successful implementation of updates will be monitored and documented through a ticketing process.

- Pre-logon banners are in place. For all future server installations, a server installation checklist will be used that includes adding a pre-logon banner.

   Target Implementation Date for OAL: September 2013.

ITSS has implemented or is in the process of implementing the following:

- Password controls now meet or exceed university policy. To assist with future enforcement, a Windows password policy will be implemented at the domain level for greater control. For Linux installations, a checklist will be used that includes
1. Logical Security (cont.)

   changing password policies. Systems will be periodically reviewed for compliance.

   - System patches are current. For continuous patch management, ITSS will begin using the same or equivalent tools and processes OAL uses.

   - Pre-logon banners are in place. For all future server installations, a server installation checklist will be used and verified that includes adding a pre-logon banner.

   **Target Implementation Date for ITSS: September 2013.**

Supercomputing, which utilizes Linux, has completed or is in the process of completing the following:

   - Implementation of password controls in accordance with university guidelines is expected to be completed by the end of September 2013. Compliance with requirements will be periodically monitored.

   - System patches are current. Patch management procedures will be reviewed for continued performance.

   - Pre-logon banners have been put in place according to university and state regulations. Compliance with requirements will be periodically monitored.

   **Target Implementation Date for Supercomputing: September 2013.**

2. Help Desk Central

   **Observation**

   Help Desk Central does not have the necessary processes and tools to ensure achievement of customer service level baselines and operational goals and objectives. For example, the CIS 2011-2015 strategic plan goal to increase the number of trouble calls that are resolved by the first person answering the phone cannot be tracked with current software tools. In addition, other measures of customer service levels are not tracked such as user satisfaction per incident or the number of resolutions per minute of time.
The operation of CIS’ Help Desk Central was recently moved to a different unit under CIS and a new manager was appointed. They are aware of these issues and are working on solutions. The main challenge is that the software tools supporting Help Desk Central operations do not provide a wide-range of needed functions. Customer inquiries originate via telephone, walk-in traffic, and email. Each origination point is supported by a different system: Keystone for email, Nortel ACD for phone calls, and a medical check-in system is used for walk-in traffic. The tools are outdated and have been extended beyond their capabilities. For incoming call routing, there is a lack of defined escalation procedures to route incidents to appropriate personnel for remediation.

As the importance of help desk services has grown worldwide, standard IT service management practices have been developed to improve help desk services. EDUCAUSE, a nonprofit association whose mission is to advance higher education through the use of information technology, has noted that IT service management practices have been adopted to some extent by over three-quarters of the universities surveyed. CIS management is looking to utilize IT service management practices to help meet their stated goals and improve overall performance. Without adequate processes and tools in place, Help Desk Central may not be able to meet its customers’ needs in the most effective and efficient manner possible.

Recommendation

Develop and implement appropriate IT service management practices including the development of goals to measure service levels in the areas of user satisfaction, first contact resolution and other relevant measures.

Establish a life cycle approach, including funding requirements, to maintain software applications that support Help Desk Central operations. This would include migration paths to alternative software tools to replace Keystone, Nortel ACD, and the medical walk-in system.

Establish criteria for incident escalation procedures across service level tiers.

Management’s Response

A Customer Support Working Group (CSWG) has been established from areas supported by Help Desk Central (HDC). Among the deliverables defined for this group are the following:
2. Help Desk Central (cont.)

- Change management and service transition recommendations.
- Incident escalation procedures.
- Incident and service request life cycle recommendations, including service level goals.
- Service and support ownership recommendations at each stage of the life cycle.
- Comprehensive set of requirements for a new ticketing solution to be selected at the conclusion of the group’s commission.

In addition to the CSWG, HDC management is working with Telecommunications to evaluate a new call center solution. Infrastructure staff is independently evaluating industry standard call center solutions as well, to mitigate the risk of slow progress with campus solutions. HDC is also evaluating niche alternatives to the medical check-in system for walk-ins. In the meantime, the business process has been modified to capture more detailed information.

Recommendations from the CSWG are expected by the end of January 2014. A final decision and implementation plan will be determined by March 2014 with final implementation completed by September 2014.
BASIS OF REVIEW

Objective and Scope

The objective of the audit was to review the processes and controls in place within Computing & Information Services (CIS) to determine if information technology resources are used in compliance with laws, policies, regulations and rules. The review of CIS focused on logical security general controls administered by three departments within CIS: Information Technology Solutions & Support, Open Access Labs, and Supercomputing. Other general control areas reviewed in selected departments included network security scanning, central help desk operations, and physical security at the open access labs and network closets. The audit period focused primarily on activities from September 1, 2011 through February 28, 2013. Fieldwork was conducted from November 2012 through March 2013.

Criteria

Our audit was based upon standards as set forth in the System Policy and Regulation Manual of the Texas A&M University System; Texas Administrative Code; Texas Information Resources Management Act; Texas A&M University Standard Administrative Procedures; and other sound administrative practices. This audit was conducted in conformance with the Institute of Internal Auditors’ “International Standards for the Professional Practice of Internal Auditing.”

Additionally, we conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

CIS is one of seven departments under the Vice President and Associate Provost for Information Technology and is responsible for providing computing resources, services and support to Texas A&M University students, faculty and staff, as well as other members of The Texas A&M University System. There are six units within CIS: Information Technology Solutions and Support; IT Infrastructure and
Operation; Networking and Information Security; Open Access Labs; Support Services; and Supercomputing. CIS operates as a university service center with a budget of approximately $30 million, not including student access fees, and has approximately 206 full-time employees.

AUDIT TEAM INFORMATION

Dick Dinan, CPA, Director
David Maggard, CISA, Audit Manager
Paul Wiggins, CISSP
Bill Williams, CISA

DISTRIBUTION LIST

Dr. R. Bowen Loftin, President
Dr. Karan Watson, Provost and Executive Vice President for Academic Affairs
Ms. B.J. Crain, Vice President for Finance and Chief Financial Officer
Dr. Rodney McClendon, Vice President for Administration
Dr. Pierce Cantrell, Vice President and Associate Provost for Information Technology
Dr. Pete Marchbanks, Executive Director – Computing and Information Services
Mr. Charley B. Clark, Associate Vice President for University Risk and Compliance