Overall Conclusion

Overall, the controls established over the primary learning management system at Texas A&M University, Blackboard Learn (eCampus), are effective in providing reasonable assurance that the information in the system is accurate, complete, available, and in compliance with related laws, policies and regulations except in the area of logical security controls. Several weak logical security practices were noted. Improvements are also needed in the areas of password controls within the eCampus application and change management practices outside of the normal change management process.

The Instructional Technology Services (ITS) department is responsible for all aspects of eCampus support and has developed several practices that provide for more efficient operations. These practices include utilizing the university’s central authentication system for faculty and student account access and automated interfaces with the Compass student information system for setting up courses and populating students into their respective classes in eCampus. Additional efficiencies could be gained by requiring the two academic departments that currently use two other learning management systems to utilize eCampus instead.

Summary of Significant Results

Logical Security

Administration and oversight of logical security requires improvement to strengthen the controls in place to protect the eCampus system and its data. Several weak logical security practices were noted in the areas of software lifecycle management, pre-logon banner use, and password management. These weaknesses increase the university’s risk for the disruption of critical information technology (IT) services and the compromise of information.
Summary of Management’s Response

*Instructional Technology Services (ITS) promotes and enables the effective use of technology in teaching and learning. We strive to provide a reliable, secure and efficient learning management system for all of the university community to use. The recommendations detailed in the audit report will further enhance the department’s administrative processes. Actions are being taken to address the audit recommendations and the department will continue to work with the Provost and university community in adopting the centrally supported learning management system. Detailed responses are included in each section.*
Detailed Results

1. Logical Security

Improvements in logical security controls are needed to increase overall IT security. Logical security for eCampus was reviewed on select systems administered by ITS and Computing and Information Services (CIS). These systems included nine Linux servers (five Red Hat Enterprise Linux (RHEL) and four SUSE Linux Enterprise Servers (SLES)), a Windows server, and three databases (two Oracle and one Microsoft SQL Server). Several weak logical security practices were noted in the areas of software lifecycle management, pre-logon banner use, and password management. The following specific logical security weaknesses were noted:

- Various issues were noted on the SLES systems. All four are no longer supported by the vendor due to not having a supported service pack installed. In addition, all four did not enforce password construction requirements for local accounts and three did not have a Texas Administrative Code (TAC) 202.75 compliant pre-logon banner in place. For two of these four systems, responsibility for system administration was not clearly defined between ITS and CIS such that neither were monitoring these systems. The departmental agreement between ITS and CIS expired on August 20, 2013 and had not been renewed. The agreement did not clearly indicate which party was responsible for each system. The issues noted on the other two SLES systems were due to the lack of custodian oversight.

- The Microsoft SQL database server that was tested is no longer supported due to not having a supported service pack installed. This was due to the lack of custodian oversight caused primarily by it being an individual/one-off database server and not part of CIS’ managed database cluster. The two Oracle databases tested were found to not have critical patch updates installed in a timely manner. These updates are released quarterly, but gaps existed in their installation of nine and twelve months. The Oracle database patching issues were due to not having regularly scheduled quarterly maintenance windows for the Oracle databases. eCampus is a mission-critical system and scheduling downtime for maintenance was a concern for ITS.

- Password practices for a number of the tested systems that support eCampus do not meet university standards. For the five RHEL servers tested, if password criterion were active, not all existing accounts had been required to change their passwords in order for the new rules to be applied. In addition, we were able to discover at least one account password on each machine. In
each of these cases, password construction did not meet university standard administrative procedures and the passwords appear to be default Blackboard passwords. Each of these accounts had the ability to elevate their privileges to that of super-user access that could have been gained by using a default password. It was noted that the default passwords were not changed after installing the related application as the custodians were reluctant to change them because they did not know how future updates and patches might be impacted. For the Oracle databases tested, none enforced a university-compliant password policy and one account password was discovered on each system. The poor password construction for the Oracle database accounts was due to the absence of password complexity controls.

TAC, Chapter 202, and Texas A&M standard administrative procedures provide requirements related to the establishment of strong general IT controls including software lifecycle management, pre-logon banner use, and password management. Failure to follow strong general IT practices can lead to files or systems being compromised resulting in the loss or theft of data and/or equipment and the possible disruption of services through either equipment failures or unexpected events.

**Recommendation**

Implement a more rigorous software lifecycle management program that includes operating systems and applications and develop monitoring processes for compliance. Patches should be implemented within 90 days of release, with the exception of critical security vulnerability patches that should be applied immediately. Service packs should be implemented before the previous service packs become unsupported. This will require coordination between CIS and ITS to balance the security and functionality issues that patches/updates address and the issue of maintenance windows and downtime of eCampus. The process should include reporting by CIS to ITS on the status of patch updates.

Ensure that university-compliant password rules are put in place for all Linux operating systems and that affected users are then required to change their passwords. For the Linux accounts found to have default user account passwords in place, ensure that those passwords are also changed to meet university password rules.

Apply a university-compliant password verification function across all Oracle database profiles. All affected user accounts should then be required to change their password.

Execute a departmental agreement between ITS and CIS to cover the current period. Clearly establish responsibilities and expectations in writing (such as in
Management’s Response

SLES and Oracle systems have been patched to the most current version available. ITS will coordinate with CIS to upgrade the single SQL server instance to the latest SQL server version by July 2014. ITS and CIS will adopt a new software release lifecycle for SLES, RHEL, SQL, and Oracle. All patches will be implemented within 90 days of release with the exception of critical security patches which will be applied immediately. Blackboard updates will continue to follow the twice a year vendor release cycle as needed. Infrastructure updates will be communicated by CIS to ITS via email to allow time and proper communication to customers in the event of any scheduled application downtime. ITS and CIS will include the adopted software release lifecycle, monitoring, and reporting requirements within the updated service agreement effective September 2014.

Password rules have been modified to comply with university password requirements. University compliant passwords were implemented as of April 2014 on all SLES and RHEL local operating system accounts. Any unused administrative accounts have been deleted from the RHEL servers. The password for the Blackboard account used to install the application has also been changed to be in compliance with university standards for password construction.

CIS database administrators have implemented Oracle user account passwords that meet university password requirements. Oracle profiles for user accounts were implemented June 2014 that apply a university-compliant password verification function to all Oracle databases.

A pre-login banner was implemented April 2014 on all SLES systems to bring those systems into TAC 202.75 compliance.

ITS and CIS will address within the aforementioned service agreement support to be rendered and responsibilities and expectations regarding which systems or applications CIS is responsible for and which systems ITS is responsible for.

2. Application Local Accounts

The eCampus application does not have built-in local password controls to enforce university requirements related to password complexity and length. This affects the security of credentials for approximately 21 eCampus local accounts used for system administrator, remote campus access, and application support roles.
It was noted that these accounts can be directly accessed from an eCampus web address without first logging into Texas A&M’s central authentication system. This is a limitation of eCampus and will require the vendor to modify its product. The university’s Standard Administrative Procedure 29.01.03.1M1.14, Information Resources – Password-based Authentication sets the password complexity and expiration guidelines for all information resources. Failure to implement strong password practices increases the risk that sensitive files or systems could be compromised and critical services could be disrupted.

**Recommendation**

Where the eCampus vendor does not have password controls in place, communicate this oversight to the vendor and request that password controls be implemented in accordance with university procedures.

**Management’s Response**

*In February 2014, ITS confirmed with the vendor that built-in local password controls are a known learning management system application limitation. As a result, ITS submitted a product enhancement request for a built-in password control structure that would meet university password standards. The request was submitted April 2014. Additionally, ITS is investigating an alternative method for logging-in to the application that would enforce university required password controls. The alternative method will be tested and, if feasible, will be implemented by September 2014.*

3. **Change Management**

**Controls over the change management process do not adequately monitor changes that might be made outside of the established change control procedures.** ITS maintains a robust change management process that is governed by a Change Advisory Board and documented in the “Integrated Change & Release Management Plan.” However, there are no processes in place to monitor the production environment for changes that can be reconciled back to approved changes. Four individuals have the local eCampus system administrator role that allows them to make changes to all eCampus application environments including production. In addition, eCampus does not currently maintain audit logs that would facilitate the identification and reconciliation process for all changes. Unauthorized changes to the production environment could lead to unscheduled outages or risk of fraud. In order to effectively monitor and enforce the change control process, detective controls must be in place to monitor the production environment for
changes, reconcile these changes to approved changes, and report any unauthorized variance to management.

**Recommendation**

Strengthen the change control processes to monitor the production environment for all changes, reconcile these changes to approved changes, and report unauthorized variances.

**Management’s Response**

*ITS has worked diligently towards a formal change and release management process. However, there is still a need for an internal audit mechanism or process to monitor actual changes within the vendor application. ITS will review and determine if a more streamlined or automated process can be implemented to monitor system changes. The review will be completed by September 2014. In the interim, ITS will implement a manual process that involves observing system log files. The manual process will be implemented by September 2014.*

4. **Additional Learning Management Systems in Use**

Two academic departments are still maintaining separate learning management systems while all others have voluntarily adopted eCampus for traditional college credit courses. Industrial Distribution and Chemical Engineering each maintain separate systems mainly for delivering continuing education courses to non-students in addition to college credit courses. eCampus has a process available to enroll non-students in continuing education classes and appears to be meeting the overall needs of its customers. The cost of maintaining eCampus is covered through the Provost’s Office and departments are not charged for the use of the system for college credit courses. Allowing departments to maintain their own learning management systems results in increased hardware and administration costs and requires students to learn how to use an additional learning management system just for classes taken in those departments. It should be the university’s goal to operate as efficiently as possible and to streamline the student’s learning environment as much as possible.

**Recommendation**

Unless there is a compelling business need to maintain separate learning management systems, require all academic departments to utilize the university’s eCampus system.
Management’s Response

ITS will coordinate with Industrial Distribution and Chemical Engineering to document the pros and cons of implementing the centrally supported learning management system. Each department will provide a response and the Provost and Executive Vice President for Academic Affairs will approve the decision made by November 2014.
Basis of Review

Objective and Scope

The overall objective of this audit was to evaluate the general and application controls of the primary learning management system at Texas A&M University (eCampus) to determine if the information is accurate, complete, available and in compliance with related laws, policies and regulations. The review of eCampus at Texas A&M University focused on general and application controls in place. General IT controls apply to all system components, processes and data, and include logical access, system development, change management, and backup and recovery controls. Application controls are contained within the software application and are designed to ensure the complete and accurate processing of data from input through output. Examples of application controls include user identification, transaction authorization, and input and output controls. The audit period focused primarily on activities from September 1, 2013 to February 28, 2014. Fieldwork was conducted from February to April 2014.

During the period under review, September 1, 2013 through February 28, 2014, the university was transitioning from the Blackboard Vista system, branded by the university as eLearning, to the newer Blackboard Learn system, branded as eCampus. During this period, the university ran both systems in parallel to allow faculty time to transition to eCampus. eCampus was implemented and first used for the fall 2013 semester and will be the only one available starting fall 2014. Our review focused on eCampus and the new infrastructure and processes in place.

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 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.

Audit Team

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

Distribution List

Dr. Mark Hussey, Interim 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. Pierce Cantrell, Vice President and Associate Provost for Information Technology
Mr. Jim Snell, Director of Instructional Technology Services
Dr. Pete Marchbanks, Executive Director – Computing and Information Services
Mr. Charley B. Clark, Associate Vice President for University Risk and Compliance