UT DALLAS

THE UNIVERSITY OF TEXAS AT DALLAS

Office of Internal Audit 800 West Campbell Rd., SPN 32, RICHARDSON, TX 75080 (972) 883-4876

October 6, 2014

Dr. Daniel,

We have completed an audit of eLearning/Blackboard application as part of our fiscal year 2014 Audit Plan, and the report is attached for your review. The audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The objectives of the audit were to ensure adequate controls exist over eLearning/Blackboard to ensure compliance with appropriate laws, policies and procedures, the effectiveness and efficiency of operations, and the reliability and integrity of financial and operation information and the safeguarding of assets.

Overall, we found that controls within the application should be strengthened by improving information technology processes. The attached report details recommendations that will enhance compliance and internal controls.

Management has reviewed the recommendations and has provided responses and anticipated implementation dates. Though management is responsible for implementing the course of action outlined in the response, we will follow up on the status of implementation subsequent to the anticipated implementation dates. We appreciate the courtesies and considerations extended to us during our engagement. Please let me know if you have any questions or comments regarding this audit.

Toni Stephens

Toni Stephens
Institutional Chief Audit Executive

UT Dallas Responsible Parties:
Dr. Darren Crone, Director Educational Technology Services

Members of the UT Dallas Audit Committee:
External Members:
Mr. Bill Keffler
Mr. Ed Montgomery
Ms. Cynthia Trochu
Dr. Hobson Wildenthal, Executive Vice President and Provost
Dr. Calvin Jamison, Vice President for Administration
Mr. Terry Pankratz, Vice President for Budget and Finance
Dr. Andrew Blanchard, Vice President for Information Resources and Chief Information Officer; Dean of Undergraduate Studies
Dr. Bruce Gnade, Vice President for Research
Dr. Darrelene Rachavong, Vice President for Student Affairs
Mr. Timothy Shaw, University Attorney

The University of Texas System:
Dr. Pedro Reyes, Executive Vice Chancellor for Academic Affairs
Alan Marks, Attorney
Mr. J. Michael Peppers, CIA, CRMA, CPA, FACHE, Chief Audit Executive
Ms. Moshmee Kalamkar, CPA, CIA, Audit Manager

State of Texas Agencies:
Legislative Budget Board
Governor's Office
State Auditor's Office
Sunset Advisory Commission

Executive Summary

eLearning, Report No. 1502

Audit Objective and Scope: To ensure adequate controls exist over eLearning/Blackboard to ensure compliance with appropriate laws, policies and procedures, the effectiveness and efficiency of operations, and the reliability and integrity of financial and operation information and the safeguarding of assets.

Audit Results:
The audit resulted in no recommendations considered priority, or significant to University operations. However, we offer the following recommendations to enhance compliance and internal controls over eLearning operations:

Recommendations	*Estimated Implementation Date*
(1) Secure FERPA Protected Data	June 19, 2014
(2) Improve Integration Security	December 1, 2014
(3) Maintain System and Information Integrity	December 1, 2014
(4) Strengthen Database Controls	December 1, 2014
(5) Improve Authentication Controls	December 1, 2014
(6) Implement Building Blocks Controls	*will not implement*
(7) User Access Management	March 1, 2015
(8) Operational Efficiency	April 1, 2015
(9) Audit Logging	December 1, 2014
(10) Develop Policies and Procedures Manual	September 1, 2015

Conclusion: Controls within the eLearning application should be strengthened. Implementation of the recommendations outlined in this report will help the enhance controls and compliance with applicable policies and procedures.

Responsible Vice President:	**Responsible Party:**
Dr. Hobson Wildenthal, Executive Vice President and Provost; Dr. Andrew Blanchard, Vice President for Information Resources and Dean of Undergraduate Studies	Dr. Darren Crone, Director Educational Technology Services

Staff Assigned to Audit:
Ali Subhani, CIA, CISA,GSNA, IT Audit Manager; Colby Taylor, IT Staff Auditor; student interns from the Internal Auditing Education Partnership Program at the Naveen Jindal School of Management: Arpitha Kaushik and Prateek Varshney

Table of Contents

Background

Educational Technology Services (ETS), within the Office of the Provost, is responsible for administering the Blackboard Learn application on campus. At UTD, the Blackboard Learn application is known as the eLearning System (ES). The ES is utilized for delivering course content and allows for collaboration between students.

The ETS Director, who reports to the Dean of Undergraduate Studies, leads the ETS department. The department is split into three divisions; eLearning Services, Video Services, and Media Services. This audit focused only on the eLearning Services division. In addition, there are two employees within the Enterprise Architecture Services (EAS) department in Information Resources that provide technical expertise to support the ES.

At the beginning of the fiscal year, the eLearning Services division was comprised of nine full-time employees and five student workers. The division has an operating budget of $1.3 million. $741,000 from the budget is allocated to contracts for major applications such as Blackboard Learn, Turnitin, and Qualtrics. Additionally, the salary for the System Administrator that supports the Blackboard Learn application is paid by Information Resources (IR).

Audit Objective

To ensure adequate controls exist over eLearning/Blackboard Learn application to ensure compliance with appropriate laws, policies and procedures, the effectiveness and efficiency of operations, and the reliability and integrity of financial and operation information and the safeguarding of assets.

Scope and Methodology

The scope of this audit was Fiscal Year 2014 to date, and our fieldwork concluded on September 30, 2014. The Media Services and Video Services divisions of the department were not in scope for this audit. To satisfy our objectives, we performed the following:

- Interviewed personnel to gain an understanding of the Blackboard Learn application.
- Reviewed the contract with the vendor that is hosting the Blackboard Lean application
- Gained an understanding of the process through which student, faculty, staff and course data was imported into the Blackboard Learn application.
- Evaluated authentication controls within the application and the database.

- Reviewed data security controls.
- Evaluated security privileges for users. Special attention was placed on security privileges that allowed access to Family Educational Rights and Privacy Act (FERPA) data.
- Reviewed controls around Building Blocks TM. Building Blocks are mini applications that run within the Blackboard Learn application.
- Reviewed integration security. Integrations are the data transfer points between different applications.
- Analyzed current processes to identify opportunities to improve efficiency.

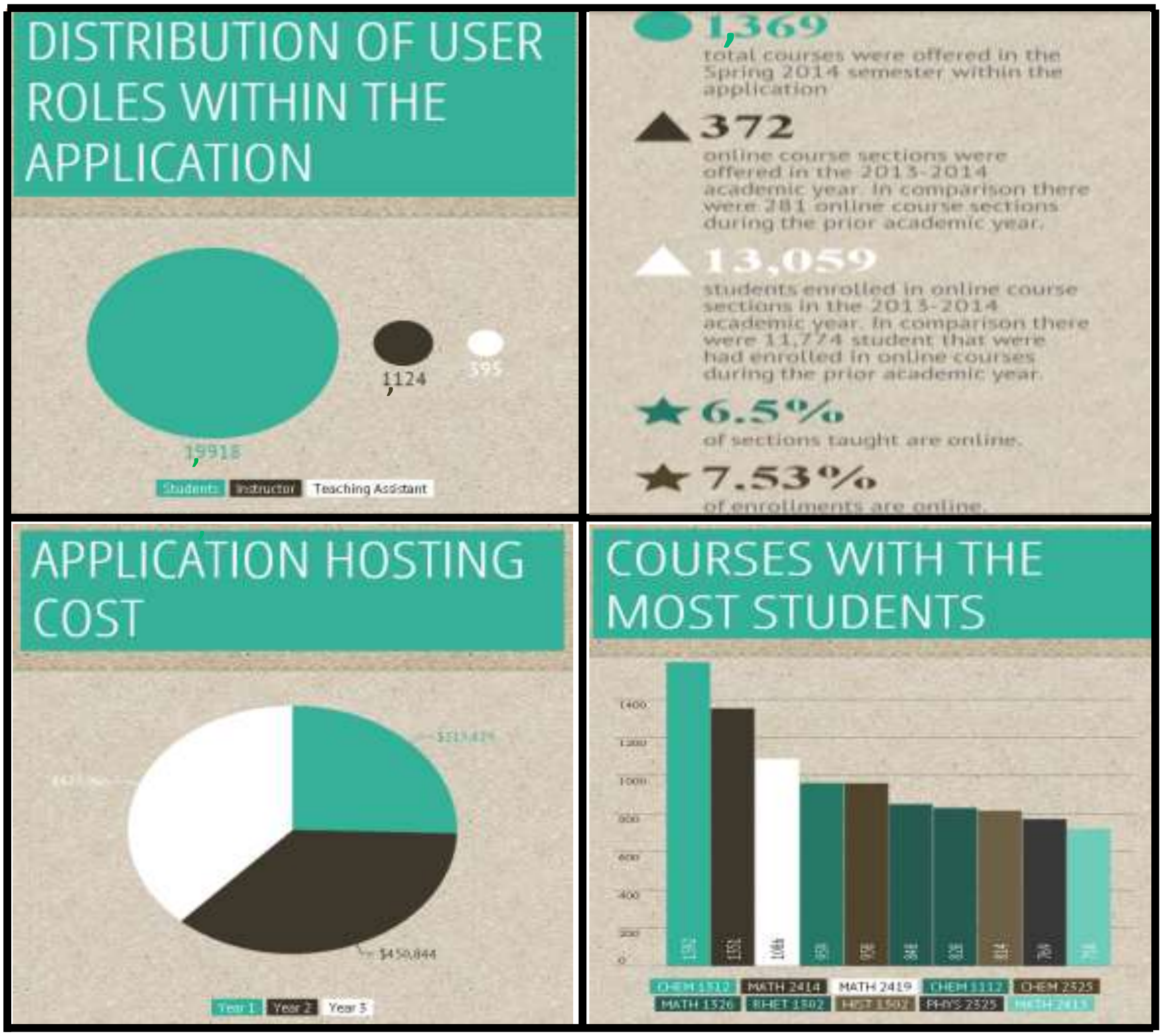
Where applicable, we conducted our examination in accordance with the guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing*. The *Standards* set criteria for internal audit departments in the areas of independence, professional proficiency, scope and performance or audit work, and management of the internal auditing department.

Audit Results and Management's Responses

Overall, we found that controls over the ES can be strengthened. Our audit work indicated that the following controls currently exist:

- Access logs exist to identify users that are logging into the application.
- An authentication process for non-local user accounts is functioning as intended.
- Application data is appropriately being encrypted in transit.
- Configurations are enabled to limit course size.
- A process to export data from the PeopleSoft Student System into Blackboard currently exists.
- A maintenance schedule is in place during non-peak hours to minimize the impact on the user community.
- A process to archive course material from prior semesters currently exists.
- Data that is communicated via the integration process is being encrypted.
- Functionality within the application to safeguard against unsafe Hyper Text Markup Language (HTML) is currently being utilized. HTML is the language that is utilized to create web pages or course content for the ES.
- An automated process exists to disable student access to course material after the semester has ended.

The following table visually depicts data that was gathered during the audit process:



DISTRIBUTION OF USER ROLES WITHIN THE APPLICATION

1,369 total courses were offered in the Spring 2014 semester within the application

372 online course sections were offered in the 2013-2014 academic year. In comparison there were 281 online course sections during the prior academic year.

13,059 students enrolled in online course sections in the 2013-2014 academic year. In comparison there were 11,774 student that were had enrolled in online courses during the prior academic year.

6.5% of sections taught are online.

7.53% of enrollments are online.

APPLICATION HOSTING COST

COURSES WITH THE MOST STUDENTS

Audit Recommendations

A priority recommendation is defined as one that may be material to operations, financial reporting, or legal compliance. This would include an internal control weakness that does not reduce the risk of irregularities, illegal acts, errors, inefficiencies, waste, ineffectiveness, or conflicts of interest to a reasonable low level. We have **no priority recommendations** resulting from this audit; however, the following recommendations will help strengthen information technology processes.

(1) ***Secure FERPA Protected Data***

Under FERPA[1], "*a school may not generally disclose personally identifiable information from an eligible student's education records to a third party unless the eligible student has provided written consent."* During the audit the following files were identified that were not secured adequately:

File Name	Designated File Owner	Date Created	File Size
ENROLL_STUDENTS_2014-01-07_15-53-31_.xml	Educational Technology Services	*Jan 7,2014*	*3,685,082 KB*
ENROLL_STUDENTS_2014-01-12_20-13-41_.xml	Educational Technology Services	*Jan 12, 2014*	*6,023,489 KB*
ENROLL_STUDENTS_2014-01-14_16-41-06_.xml	Educational Technology Services	*Jan 14,2014*	*6,597,624 KB*
PROD_MEMBERSHIP2145.XML	Educational Technology Services	*Apr 28,2014*	*10,390,913 KB*
PROD_PEOPLE2145.XML*	Educational Technology Services	*May 1, 2014*	*4,665,716 KB*

The files were accidentally assigned world read, write, and execute privileges. Additionally, the folder that the files were saved in had the execute privilege for the world. As a result, the files could potentially be accessed by approximately 2,500 individuals with accounts within the UNIX environment at UTD, based on analysis by the Unix Manager. This could only occur if the individuals attempting to access the files were knowledgeable about the complete file names above.

Recommendation: Security privileges for the files should be adjusted so that only individuals with a valid business have access to the FERPA protected data. Additionally, a periodic review of the security privileges should be performed for folders where FERPA protected data specific to the ES is temporarily stored.

Management's Response: *This has been implemented. The directory can no longer be accessed by anyone other than the programmer. Read, Write, and Execute have been removed from the directory.*

Estimated Date of Implementation: *June 19, 2014*

[1] http://www2.ed.gov/policy/gen/guid/fpco/ferpa/students.html

Person Responsible for Implementation: *Corinne Griffin, Programmer Analyst EAS*

(2) ***Improve Integration Security***

In order for the ES to function, integration(s) must be set up to transport data from the PeopleSoft Campus Solutions (PCS) into ES. During a review of the integrations that were in place to transport data between the two applications, the following deficiencies were noted:

- The username and password that is required to upload data into the ES was saved in a file on the home directory of the system administrator that supported the application. The file was not encrypted. As a result the password could potentially be compromised. At the time of the audit the security privileges on the file were appropriately configured so that only the file owner could read, write, or execute the file that contained the password.
- The password that was being utilized during the integration process was not in line with university requirements for an acceptable password. However, the user name that is created is complex and unique.
- There was no process in place to periodically change the password on a set schedule.
- The integration points were configured in a manner that did not restrict access to initiate data transfer sessions from limited Internal Protocol (IP) addresses. As a result, if an individual got access to the credentials that are utilized during the integration process, they would be able to corrupt or modify data within the application without being present on campus.
- An integration that had not been utilized for an extended period of time was still active. Integration points allow access to application data so therefore they should be disabled once functionality is no longer required.

According to TAC 202.75 A[2] "*Confidential information shall be accessible only to authorized users. An information file or record containing any confidential information shall be identified, documented, and protected in its entirety*."

Recommendation:

Management should consider enhancing controls around the integration process by:

- Encrypting the file that contains the password that is utilized during the data upload process.
- Ensuring that the password that is utilized in the integration process is in line with UTD Information Security requirements. Alternatively, management should document risk acceptance if the password will not be set in line with UTD requirements.

[2] http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=75

- Implementing a process to periodically change the integration password
- Implementing controls so that the integration process can only be initiated from an authorized site/IP address.
- Removing integrations that are no longer being utilized in current business processes.

Management's Response: *1. The file will be encrypted by October 1, 2014. 2. The password will not be changed to be in line with university standards due to the inability to change Blackboard default password settings. Management will document risk acceptance by December 1, 2014. 3. A notification process (using calendar reminders) will be put in place to change the password every 6 months by December 1, 2014. 4. TBD. Programmer will meet with Blackboard and UTD Unix Group to determine the feasibility of changing the process so it can only be initiated by an authorized site/IP address by December 1, 2014. 5. Integrations not used for 6 months will be made inactive by December 1, 2014. This process will be included in the documentation*

Estimated Date of Implementation: *December 1, 2014*

Person Responsible for Implementation: *Corinne Griffin, Programmer Analyst EAS; Darren Crone, Director of ETS*

(3) ***Maintain System and Information Integrity***

According to TAC 202.75 7 Y,[1] "*Malicious Code--Describes the requirements for prevention, detection, response, and recovery from the effects of malicious code (including but not limited to viruses, worms, Trojan Horses, and unauthorized code used to circumvent safeguards).*" Prior to signing the contract with the vendor that hosts the ES, the Information Security Office (ISO) required that a vendor survey be completed. This allowed the former Director of ISO to perform a security assessment of the application. Once the survey was completed by the vendor, it was directly routed to the ISO. The Director for ETS was informed by the former Director of ISO that the vendor had passed the security review and that the department could proceed with the purchase of the application.

In Internal Audit's review of the survey, it was noted that the vendor indicated that "*Currently there is no virus protection on the servers*" that host the application. According to the Director for ETS, the vendor stated the reason there is no virus protection is due to the negative impact virus scanning has on performance of the system. The current Director of ISO helped validate with the vendor that any malicious files uploaded by students or faculty members would not likely be executed on the server or negatively impact ES. However, malicious file(s) could negatively impact the

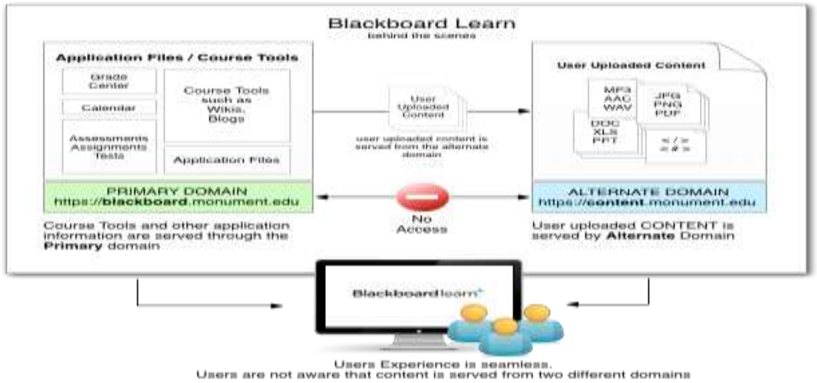
[1] http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=75

ES if content is uploaded using accounts that have administrative privileges on the server. It is the vendor's responsibility to develop controls around administrative accounts. Development of anti-virus scanning capability on files uploaded by users has been on the vendor's roadmap since January 1, 2013; however, there is currently no anticipated target date for implementing this functionality.

Also, no documentation detailing the risk acceptance by UT Dallas management was available. The former ISO did not require or request a risk acceptance. Also, given the fact that the users that utilize the application regularly upload files into the application, there is increased likelihood for viruses to be distributed to the campus infrastructure once faculty or teaching assistants download the assignment material on their workstations for review, especially when those workstations do not have anti-malware protection or current patches installed.

Additionally, the following opportunity to further enhance system configuration was noted: Rendering user-uploaded files from an alternate domain is a defense-in-depth security control that is recommended by the application vendor as a best practice. By uploading a piece of content containing potentially malicious scripts, a user could potentially perform session hijacking on the main ES session once a target user accesses the affected content. The configuration that offered a method of protection against this type of activity was currently not enabled as there would be additional hardware that would be required to fully implement the configuration.

Depiction of Separate Domain for Rendering Content


Blackboard Learn
behind the scenes
Application Files / Course Tools
Grade Center
Calendar
Assessments Assignments Tests
Course Tools such as Wikis, Blogs
Application Files
PRIMARY DOMAIN
https://blackboard.monument.edu
Course Tools and other application information are served through the Primary domain
User Uploaded Content
user uploaded content is served from the alternate domain
No Access
User Uploaded Content
MP3 AAC WAV
JPG PNG PDF
DOC XLS PPT
< / > = # =
ALTERNATE DOMAIN
https://content.monument.edu
User uploaded CONTENT is served by Alternate Domain
Blackboardlearn+
Users Experience is seamless.
Users are not aware that content is served from two different domains

[3]

[3] https://help.blackboard.com/en-us/Learn/9.1_2014_04/Administrator/070_Server_Management_and_Integrations/Security/000_Key_Security_Features/System_and_Information_Integrity/000_Safer_Dynamic_Content_Rendering

Recommendation: Management should formally document that they have accepted the risk of the vendor not implementing virus scanning capability on the server supporting the application and document controls in place that would reduce these risks. Additionally, training should be offered to faculty, staff, and technical personnel that utilize the application to stress the importance of ensuring that they only access the ES from a device that has an up-to-date anti-malware scanner and current patches installed. Lastly, management should consider implementing an alternate domain for uploading user content.

Management's Response: 1. The risk of not implementing virus scanning was considered and accepted by Information Security prior to implementation of the system. Representatives from the vendor indicated that they were not aware of any virus issue from user uploaded content. Management will document that they have also accepted the risk by December 1, 2014. 2. Training sessions will include a discussion on the importance of using only devices with current virus scanners to upload to the Learning Management System by December 1, 2014. UTD currently has policies in place that includes the use of anti-malware tools for workstations. 3. Management has researched the feasibility of implementing an alternate domain for uploading user content. Based on the analysis performed there is concern that by adding additional components/processes, there will be another point of failure introduced into the system, potentially adversely impacting the end user. As a result management has decided not to implement a separate domain for rendering content

Estimated Date of Implementation: December 1, 2014

Person Responsible for Implementation: *Darren Crone, Katrina Adams*

Auditor Comment: Documentation was not made available, and may not exist, to demonstrate whether ISO brought this risk to the attention of the eLearning team nor to demonstrate that eLearning team leadership accepted that risk.

(4) ***<u>Strengthen Database Controls</u>***

According to TAC 202.75 4 (A),[4] *"Confidential information that is transmitted over a public network (e.g.: the Internet) must be encrypted*." During the audit it was noted that the ES was not encrypting communication at the database layer during data exchange. Currently there is one user with the ability to query information from the database directly. The ES was implemented in 2012. Currently, responsibilities for managing the security of the ES are divided among the following groups:

- **Educational Technology Services**: responsible for ensuring that access rights for individuals within the application are being managed appropriately.

[4] http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=75

- **Application Vendor**: responsible for ensuring physical and logical security of the environment where the application is hosted.
- **UTD Information Security Office:** responsible for ensuring security of the UTD network that is used for communicating data between UTD and application vendor.

Additionally it was noted that before a user would be allowed to make a database connection, a firewall at the vendor's site verifies that the request is coming from an authorized IP address. The IP address that was provided to the vendor during the configuration of the database is assigned to all outgoing network traffic that originates from a particular building at UTD. As a result, any individual within the building at UTD would be able to initiate a connection to the database as they would not be blocked by the firewall rules that are in place. The individual would still be required to provide the correct user name and password in order to complete the connection request and successfully logon to the database.

Recommendation: The database configuration should be changed to ensure that communication only occurs over a secure protocol and that only Information Resources personnel are able to make a successful connection to the database.

Management's Response: 1. The Programmer will open a ticket with Blackboard to determine what changes can be made to the database configuration so communication only occurs over a secure protocol by December 1, 2014. 2. The Programmer and Director will work with IR Management to determine feasibility of having a static IP address assigned to her by December 1, 2014. Item 2 will not be immediately addressed as IR processes regarding IP addresses are being re-evaluated.

Estimated Date of Implementation: December 1, 2014

Person Responsible for Implementation: *Corinne Griffin, Darren Crone*

(5) ***Improve Authentication Controls***

Adequate authentication controls are vital for safeguarding and maintaining the integrity and availability of the institution's key information technology infrastructure. According to TAC 202.75 d),[5] "*Information resources systems which use passwords shall be based on industry best practices on password usage and documented institution of higher education risk management decisions*." Additionally, according to UTD Information Security Manual,[6] "*Passwords for accounts associated with Category I, II & III data types (see Data Classification Standards): Must:*

- *Be at least eight characters in length.*

[5] http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&ti=1&ch=202&rl=75
[6] http://www.utdallas.edu/infosecurity/documents/SecurityOperationsManual.pdf

- *Contain at least three of the following within the first 8 characters: upper case letters, lower case letters, numbers, and special characters (e.g. ! @ # $ % & * ( ) - + = < >)*
- *Be changed semi-annually."*

Due to limitations in the ES, a password configuration to control accounts that were directly (local) setup with the application did not exist. As a result, a business process that requires users with admin accounts to create passwords that are in line with the requirements of the UTD Information Security Manual currently does not exist. Additionally, the password configuration for the reporting database was also not in line with requirements of the UTD Information Security Manual. IR and ISO are currently in the process of developing a strategy for utilization of new technologies that offer dual authentication mechanisms for critical infrastructure. Once implemented dual authentication mechanisms could also be implemented for privileged users within the ES. No timeline for implementation is currently in place.

Recommendation: Management should ensure that authentication controls in application and the database within the Blackboard environment are in line with best practices and requirements of the UTD Information Security Operations Manual.

Management's Response: 1. Users with administrative accounts will be contacted and instructed on how to change passwords to be in line with UTD Information Security standards. This notification will be sent out every 6 months beginning December 1, 2014.

Estimated Date of Implementation: December 1, 2014

Person Responsible for Implementation: *Katrina Adams*

(6) ***Implement Building Blocks Controls***

According to TAC 202.75 7 U, [7] "*Platform Management--Establishes the requirements and the procedures for installing, configuring, maintaining, patching, and monitoring the integrity of a platform in a secure fashion."* The ES allows additional functionality to be implemented by installing Building Blocks™ (BB). Inadequate management of the BB's may put personal data that is protected by FERPA at risk, since the BB's may have privileges to access personal data depending on how they were configured. During a review of the BB's that had been implemented in the production environment, the following observations were made:

- 32% of the BB's that were installed did not have the most current version installed. According to the system administrator, none of the updates were

[7] http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&ti=1&ch=202&rl=75

critical or security-related updates. According to the system administrator a process was in place to evaluate whether installation of particular Building Blocks could be delayed within the production environment until the institution had the opportunity to perform testing of the BB's within the testing environment.

- A process to formally document approval of the third-party BB's to access data at the time of installation did not exist. ISO has a vendor review process in place that is required to be completed prior to any data being provided to an external vendor. However, documentation detailing ISO's review could not be located for all the third-party BB's that were currently installed. Additionally, documentation detailing the data owner's approval to provide access to data by the BB's was also not found.

Recommendation: Management should ensure that controls around Building Blocks are implemented by:

- Conducting periodic reviews to ensure that all BB's that are installed are up to date with the most current version that is offered by the BB vendor.
- Performing an analysis of security privileges for BB's that are retained and documenting acceptance of risk involved in sharing personally identifiable data with the vendor that has developed the BB. For future installs, the approval of the data owner should also be documented on the 'Implied Blackboard Data Privilege' report.

Management's Response: *1. Building Block updates are reviewed and tested each semester to determine if safe to install on production. All security and critical updates are immediately implemented. The delayed implementation of the most current version of non-critical Building Blocks is intentional, as this is done to avoid being on the "bleeding edge" and our end users experiencing bugs. 2. Information Security approved the "out of the box" building blocks when the system was implemented. The eLearning team currently works with Information Security prior to the implementation of new building blocks.*

Estimated Date of Implementation: *Will not be implemented*

Person Responsible for Implementation: *Will not be implemented*

(7) ***User Access Management***

In order for there to be sound internal controls, access privileges for users should be in line with their current job duties. During the review of access privileges that were currently set up in the application, the following observations were made:

- A timely process to disable access to course content that is provided through the Course Builder, Course Coordinator, Grader, Instructor, Teaching Assistant or the Teaching Intern roles does not exist. As a result, individuals maintain the privileges that are provided with the roles for a period of one year after the semester has ended. The roles are removed after the year has passed.
- One employee was noted as having maintained administrative privileges within the application even though the individual had transferred to another department on campus.
- Access privileges requests are not being consistently documented or tracked in a tool. As a result, it is not possible to determine if adequate authorization exists for privileges that are currently assigned to individuals.
- The vendor hosting the application is not consistently removing accounts that are being created for troubleshooting. Five accounts with different privileges were noted as being active in the application, when the accounts should have been disabled. Additionally, the vendor is only provided accounts that have generic names. As a result, accountability is diminished.
- The Instructor role provided the ability to enroll and batch enroll users into a course. The Teaching Assistant role provided the ability to enroll users into a course. As a result, individuals with the role could directly enroll users into a class and assign any security role to them within the course. Instances where individuals that were not serving as faculty members during the semester but were assigned the instructor role within the course were noted during the audit.
- At least two employees were provided System Support II roles so that they could perform job duties in the event the System Administrator was unavailable. The access roles provided privileged access that included the ability to view passwords utilized during the integration process.

A complete listing of instances where security privileges could be further limited was shared with the ETS team.

Recommendation:
The user access management process should be enhanced by:

- Implementing a process to document the privilege request and the subsequent approval prior to adjusting privileges.
- Enhancing the termination process so that privileges are terminated in a timely manner when they are no longer required.
- Documenting risk acceptance associated with creating generic named accounts for the vendor.

- Improving the role design so that users only have the ability to perform tasks that are part of their job responsibly.

Management's Response: *1. A webform and database will be created to document privilege requests. Requests will be approved by an eLearning Manager. This will be implemented by March 1, 2015, provided all dependent resources and systems can be coordinated. 2. There will be a yearly privilege review conducted. Users no longer needing those privileges will have them terminated. This process will begin March 1, 2015. 3. eLearning management will require the vendor to not use generic accounts by Aug 1, 2014. Role design modifications will be discussed with the vendor by Aug 1, 2014.*

Estimated Date of Implementation: *March 1, 2015*

Person Responsible for Implementation: *Katrina Adams, eLearning Manager*

(8) ***Operational Efficiency***

During the audit the following opportunities for improving operational efficiency were noted:

- Oracle's PeopleSoft Enterprise Student Administration Integration Pack (SAIP) allows institutions to more efficiently integrate and manage their administrative and teaching and learning systems on campus. Currently, SAIP is not implemented at the institution, and as a result there are limitations on the type of data that can be electronically transferred between the PCS and ES. For example, currently grades have to be manually entered into the PCS application even though the final course grades usually exist within ES. UT System recently approved licensing for SAIP on May 31, 2014.
- The system administrator for the ES currently does not have access to the full database suite due to cost constraints. As a result, the administrator is limited in the data that she can query which limits her ability to carry out tasks.

Best practices would suggest implementing technologies that improve operational efficiencies so that limited resources can be adequately utilized.

Recommendation: Management should consider prioritizing implementation of the technologies that will further enhance operational efficiency

Management's Response: *1. SAIP will be implemented by April 1, 2015. 2. The implementation of OpenDatabase will be taken into consideration for future budgets. The tool will be reviewed by the programmer and a recommendation made to management by December 1, 2014.*

Estimated Date of Implementation: *April 1, 2015*

Person Responsible for Implementation: *Corinne Griffin*

(9) ***Audit Logging***

The following opportunities for improvement were identified during the review of logging within the Blackboard environment:

- According to the eLearning Manager, currently logging is done by the vendor to record the user that creates local accounts or creates accounts with manual intervention within the application. However, no process is currently in place to periodically review the logs on a set schedule.
- In general, logs are being retained for a period of 30 days. According to best practices, logs should be maintained for a period long enough so that security events can be adequately investigated should the need arise.
- The LoginAs Building Block was being utilized by members of the eLearning team. The utility allowed personnel to troubleshoot errors by allowing them the capability to impersonate another user within the application. However, the same functionality can be abused to change grades for assignments. Access logs for the version of the BuildingBlock TM that was installed in the application currently do not provide the ability to easily find out who logged in as whom.

Without adequate logging, individual accountability cannot be established. According to TAC 202.75[8] *"(A) Information resources systems shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or effect the release of confidential information. (B) Appropriate audit trails shall be maintained to provide accountability for updates to mission critical information, hardware and software and for all changes to automated security or access rules*."

Recommendation: Management should work with the vendor to determine if opportunities for improvement related to audit logging that were noted can be implemented. Additionally, the LoginAs Building Blocks TM should be upgraded to the most current version that enhances logging capability. Lastly, the LoginAs Building Blocks TM logs along with the role change log should be reviewed by the Director formally to ensure the capability is being adequately utilized. The review should be formally documented.

Management's Response: *1. The programmer will discuss the inability to record sufficient logs with the vendor by December 1 2014. 2. The programmer will discuss log retention best practices with Information Security and adjust eLearning's log retention accordingly based upon the system's technical capabilities by December 1, 2014. 3. The LoginAs building block will be upgraded once it is determined that new functionality does not introduce new bugs. The director will review and document the usage of the building block by December 1, 2014.*

[8] http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=75

Estimated Date of Implementation: *December 1, 2014*

Person Responsible for Implementation: *Corinne Griffin, Darren Crone*

(10) ***Develop Policies and Procedures Manual***

The eLearning Technology Services (ETS) does not have a detailed policies and procedures manual. There is limited documentation that is available detailing certain business processes that are utilized. Departmental policies and procedures provide a clear communication of the responsibilities of departmental personnel. This is especially helpful during periods of turnover. If policies and procedures are not documented and communicated to personnel, it may lead to departmental inefficiencies and weak internal controls.

Additionally, the department has an informal process for periodically reviewing security privileges that have been assigned to employees within the application on an annual basis. According to TAC 202.71, information owners or their designated representatives are responsible for and authorized to: "*review access lists based on documented security management decisions.*" Without a formal process for reviewing security privileges that have been assigned, the department may accidentally fail to remove privileges that are no longer necessary in a timely manner.

Recommendation: Policies and procedures should be adequately documented by the department, including procedures for making changes to privileges for the Application Administrator. Additionally, the department should consider enhancing the security privilege review so that it is conducted at the end of every semester. The privilege review should be formally documented and approved by the Director.

Management's Response: *1. A policies and procedures manual will be developed and made available for initial review by September 1, 2015. 2. The enhancing of security privilege review will be conducted in the middle of each semester, beginning March 1, 2015. 3. The privilege review will be documented and approved by the director by February 1, 2015.*

Estimated Date of Implementation: *September 15, 2015*

Person Responsible for Implementation: *Katrina Adams, Corinne Griffin, Darren Crone*

Conclusion

Based on the audit work performed, we conclude that controls within the eLearning application should be strengthened. Implementation of the recommendations outlined in this report will help the enhance controls and compliance with applicable policies and procedures.

We appreciate the courtesy and cooperation received from the management and staff of the ETS during this audit.