# The University of Texas at Tyler

## Audit of Compliance with Texas Administrative Code 202

## Fiscal Year 2013

## November 2012

THE UNIVERSITY OF TEXAS AT TYLER
OFFICE OF AUDIT SERVICES
3900 UNIVERSITY BOULEVARD
TYLER, TEXAS 75799

**Table of Contents**

***Executive Summary***

The objective of the audit was to evaluate The University of Texas at Tyler (UT Tyler) internal controls over the Information Technology environment and compliance with Texas Administrative Code Section 202 (TAC 202). Adequate testing procedures have been performed to conclude that The Office of Information Resources and The University are in general compliance with the Texas Administrative Code Section 202 guidelines, except as noted in this report.

***Background***

This audit was conducted as part of the 2012 Audit Plan and is considered an "Information Technology" audit. The audit was conducted in accordance with guidelines set forth in The Institute of Internal Auditor's *Standards for the Professional Practice of Internal Auditing.* This audit is required by Texas Administrative Code (TAC) 202 to be performed biennially.

***Audit Objective***

The objective of the audit was to assess compliance with TAC 202 sections as follows:

| | |
|---|---|
| §202.70 | Security Standards Policy |
| §202.71 | Management and Staff Responsibilities |
| §202.72 | Managing Security Risks |
| §202.73 | Managing Physical Security |
| §202.74 | Business Continuity Planning |
| §202.75 | Information Resources Security Safeguards |
| §202.76 | Security Incidents |
| §202.77 | User Security Practices |
| §202.78 | Removal of Data from Data Processing Equipment |

***Scope and Methodology***

To accomplish the audit objective noted above, a risk assessment was conducted with the assistance of The University of Texas System (UT System) Audit Office liaison. Based on the assessment, the following procedures were performed as directed by the UT System Audit Office liaison:

- An internal control questionnaire (audit program) was discussed with various university personnel to determine adequacy of segregation of duties and evaluate internal controls over Information Technology (IT).
- Operations of the Information Technology and Information Security departments were evaluated to determine compliance with institutional guidelines and TAC 202 requirements.
- Additional documentation and analysis was obtained for selected high-risk areas with the primary focus on network operations.

Procedures related to Business Continuity Planning and Removal of Data from Data Processing Equipment were limited to inquiry with no detailed testing conducted.

***Audit Results***

Due to the sensitive nature of the information security function, and pursuant to Section 552.139 of the Texas Government Code, the specific observations and recommendations provided to UT Tyler management are not part of this report. Specific details of each observation and recommendation have been discussed with Information Technology and Information Security management.

**IT Development / Purchases and Related Security Requirements**

Requirements:

RULE § 202.70 (7) Security requirements shall be identified, documented, and addressed in all phases of development or acquisition of information resources.

RULE §202.75 (6) (B) Information security, security testing, and audit controls shall be included in all phases of the system development lifecycle or acquisition process.

(C) All security-related information resources changes shall be approved by the information owner through a change control process. Approval shall occur prior to implementation by the institution of higher education or independent contractors.

Observations:

University policies require that all IT projects and purchases be approved by the IT department prior to development and acquisition. This is imperative so security requirements can be identified, documented and addressed prior to development, purchase and installation. However, it was noted that the IT department is not always informed during the initial phases of projects or prior to acquisitions as required. It was also noted that university personnel occasionally purchase software without prior approval from the IT department. It was also noted that security related information resources changes were not approved in advance as required. Failure to follow the policies places the University at risk of having inadequate security or necessary funding allocated to support the IT requirements.

Recommendation:

We recommend that communication to university staff be increased to emphasize the importance of following the policies so that security requirements can be addressed timely and adequately.

Management Response and Implementation Date:

A formal process for application purchases is currently being developed. This effort is a combined effort between the Information Security Office, the Purchasing Department and the Contracts Office. The process will involve an initial information gathering questionnaire which will be completed by the requesting department. This will be followed by meetings with affected areas and the requesting department to ensure that concerns relating to security, support, contract, and purchasing are addressed prior to the purchase being approved.
Completion and Implementation Date: June 30, 2013.

**Data Identification, Controls, and Security**

Requirements:
RULE §202.71 (1) Information Owner Responsibilities. The owner or his or her designated representative(s) are responsible for and authorized to (D) specify appropriate controls, based on a risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information resources and services outsourced by the institution of higher education.

RULE §202.75 (2) (A) 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 in accordance with §202.70(1) of this chapter.

RULE §202.75 (3) (B) A user's access authorization shall be appropriately modified or removed when the user's employment or job responsibilities within the institution of higher education change.

Observations:
Confidential information is not always identified and documented, especially on network drives; therefore adequate controls may not be in place.

University policies require that the IT department be notified when an employee leaves a department or the university so access to data can be terminated. However, since there are no required exit procedures for employees changing jobs within the University or for part-time employees leaving the University, the IT department is not always notified in a timely manner. Failure to remove access increases the risk of unauthorized use and disclosure of confidential information.

Recommendation:
Information files containing confidential information should be identified, documented and protected as required.

Management Response and Implementation Date:
IdentityFinder will be used to locate files containing confidential data and users will be notified as to how to reduce the risk related to these files. Implementation Date: June 30, 2013.

Recommendation:
Stronger procedures should be developed to alert the IT department when personnel appointments change or personnel leave the University so that data access can be removed in a timely manner.

Management Response and Implementation Date:
With the implementation of the new HR/Finance system, we will look at new ways to automate the notification system so that IT knows when employees leave or transfer from one department to another. Implementation Date: December 15, 2013

## Physical Controls

Requirements:
RULE §202.73 (b) The institution of higher education head or designated representative(s) shall review physical security measures for information resources at least annually as part of the risk assessment process.

RULE §202.73 (C) Information resources shall be protected from environmental hazards. Designated employees shall be trained to monitor environmental control procedures and equipment and shall be trained in desired response in case of emergencies or equipment problems.

RULE §202.73 (D) Written emergency procedures shall be developed, updated, and tested at least annually.

Observations:
Physical security is reviewed on an on-going basis; however there is no documentation of this review.

Environmental controls and monitoring are considered adequate for the primary data center on campus, however the secondary data center does not have adequate environmental controls, monitoring or security. Failure to protect and monitor data center environmental controls could cause loss of system availability and connectivity to remote systems.

There are no written emergency procedures for the information resources in the data centers and no documented training for employees responsible for these areas. Inadequate physical controls could result in a loss of data and equipment. Failure to document and train employees to respond to emergencies could result in inefficient or inappropriate actions lengthening the time to recovery.

Recommendation:
A thorough annual review should be conducted and documented for the physical controls over information resources.

Management Response and Implementation Date:
The ISO will develop a physical controls checklist and perform annual reviews of sensitive area including University data centers & local disaster recovery sites. Implementation Date: June 30, 2013.

Recommendation:
Environmental controls, monitoring and security should be increased for the secondary data center.

Management Response and Implementation Date:
Equipment to monitor environmental and access for security including security cameras have been purchased and are pending installation and set up. Implementation Date: January 31, 2013.

Recommendation:
Written emergency procedures and documented training should be developed to protect the information resources. The procedures and training should include personnel in the physical plant and campus security departments.

Management Response and Implementation Date:
Emergency procedures and documentation for training will be developed by IT staff. These procedures will include responsibilities and notifications of personnel in the physical plant and campus security departments. Implementation Date: June 30, 2013.

## Business Continuity Planning

Requirements:
RULE §202.70 (6) Information resources shall be available when needed. Continuity of information resources supporting critical governmental services shall be ensured in the event of a disaster or business disruption.

RULE §202.74 (a) Business Continuity Planning covers all business functions of an institution of higher education. It is a business management responsibility. Institutions of higher education shall maintain written Business Continuity Plans that address information resources so that the effects of a disaster will be minimized, and the institution of higher education will be able to either maintain or quickly resume mission-critical functions. Elements of the plan for information resources shall include:

1) Business Impact Analysis to systematically assess the potential impacts of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from various events or incidents,
2) Risk Assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action,
3) Implementation, testing, and maintenance management program addressing the initial and ongoing testing and maintenance activities of the plan, and
4) Disaster Recovery Plan.

Requirements for each element are included in TAC 202.74

Observations:
The University has a Business Continuity Plan; however, the plan does not include all the requirements for each element. Elements of the plan have not been tested to ensure continuity of information resources, and the Disaster Recovery Plan for the Office of Networks and Operations has not been updated since December 2009. Failure to maintain a comprehensive, tested and updated plan could prevent the University from maintaining or quickly resuming mission critical functions.

Recommendation:
The Information Technology and Information Security departments should update the Business Continuity Plan sections related to Information Technology and Security to include all the requirements for each element of the plan.

The plan should be tested where cost effective to do so.

Management Response and Implementation Date:
The IT and Information Security departments will work together to update the required Business Continuity Plan sections. The BCP and Disaster Recovery Plans for Networking and Operations will be updated. Testing and procedures that can be performed in a cost effective manner will be developed and implemented by the Network and Operations department. Implementation Date: June 30, 2013.

**Risk Management and Assessments**

Requirements:
RULE §202.70 (4) Risks to information resources shall be managed. The expense of security safeguards shall be commensurate with the value of the assets being protected.

RULE §202.72 (a) A risk assessment of information resources shall be performed and documented. The risk assessment shall be updated based on the inherent risk. The inherent risk and frequency of the risk assessment will be ranked, at a minimum, as either "High," (annual assessment) "Medium," (biennial assessment) or "Low," (biennial assessment) based on described criteria.

(c) Risk assessment results, vulnerability reports, and similar information shall be documented and presented to the institution of higher education head or his or her designated representative. The institution of higher education head or his or her designated representative(s) shall make the final risk management decisions to either accept exposures or protect the data according to its value/sensitivity. The institution of higher education head or his or her designated representative(s) shall approve the security risk management plan.

Observations:
The University has a documented risk assessment of information resources; however the assessment is not current or inclusive of all requirements. An outdated / incomplete assessment could result in risks that are not properly addressed.

Recommendations:
The University should update the risk assessment to include all requirements so that risks can be identified and managed. The assessment should be documented and presented to appropriate management to be used in final risk management decisions so adequate security safeguards can be implemented commensurate with the value of the assets being protected.

Management Response and Implementation Date:
One of the findings in the Deloitte & Touche Security review was to update the Risk Assessment Process. This was a centralized finding and UT System is going to provide a centralized solution for this. UT Tyler will continue to use the current risk assessment process until a solution is provided by UT System. Implementation Date: UT Tyler will implement new centralized Risk Assessment process in a timely manner as it is made available.

***Conclusion***

The Information Technology function appears to comply with UT Tyler policies and procedures, state and federal guidelines and the Texas Administrative Code Section 202 with regards to Information Technology security, except as noted above. We have discussed the audit results with the appropriate personnel, and they have agreed to implement the above recommendations. We appreciate the assistance the University of Texas System Audit Office and University of Texas at Tyler personnel provided to the Audit Services Department during this engagement.

Lou Ann Viergever

Lou Ann Viergever, CPA, CIA
Executive Director of Audit and Consulting Services