Office of Internal Audit

January 3, 2017

Mr. Mark McGurk, CPA
Vice President for Business Affairs
The University of Texas of the Permian Basin
4901 E. University Boulevard
Odessa, Texas 79762

Dear Mr. McGurk:

We have completed our audit of UT Permian Basin's (UTPB) compliance with information security standards as required under Texas Administrative Code, Title 1, Part 10, Chapter 202, on information security standards (TAC 202). This audit was performed as part of our FY 2016 Audit Plan and was conducted in accordance with guidelines set forth in UTS129 and the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing.*

The objective of our audit is to determine if the UTPB information resources security program complies with the information security standards prescribed by TAC 202 and to satisfy the requirements for a biennial compliance review of the information security program pursuant to Rule 202.76(c). The audit focused on determining compliance with the Texas Department of Information Resources (DIR) Security Standards Catalog, as required by TAC 202 rule §202.76(c).

Based on the audit procedures performed, UTPB is not in full compliance with TAC 202, Rule §202.76, Security Control Standards Catalog. This resulted in one high risk finding as noted in the attached report.

We wish to express our appreciation to the management and staff of UTPB for the courtesy and cooperation extended to us during this audit.

Sincerely,

Glenn Spencer

Glenn Spencer, CPA
Institutional Chief Audit Executive

cc: Dr. David Watts, President
Mr. Steven Larizza, Chief Information Security Officer
Mr. Lowell Ballard, Chief Information Officer

The University of Texas
of the Permian Basin

FY 2016 TAC 202 – Audit Report

December 2016

Office of Internal Audit
4901 E. University
Odessa, Texas 79762

Table of Contents

Executive Summary 3

Background 3

Audit Objective 3

Scope and Methodology 3

Ranking Criteria 4

Audit Results 4

Status of Prior Year Findings and Recommendations 6

Conclusion 6

Appendix A 7

Executive Summary

The UT Permian Basin (UTPB) Office of Internal Audit has completed its audit of compliance with information security standards as required under Texas Administrative Code, Title 1, Part 10, Chapter 202, on information security standards (TAC 202). This audit was performed as part of our FY 2016 Audit Plan and was conducted in accordance with guidelines set forth in UTS129 and the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing.*

During the course of our audit, we noted that the UTPB information resources security program is not in full compliance with the mandatory information security standards found in TAC 202 rule §202.76(c), of the Texas Administrative Code (Finding No. 1).

Background

TAC 202 outlines mandatory information security controls to be implemented by all State agencies and institutions of higher education. Rule §202.76 further requires that a review for compliance with specified control standards "be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program." This audit is intended to meet that requirement for The University of Texas of the Permian Basin (UTPB).

Audit Objective

The objective of our audit is to determine if the UTPB information resources security program complies with the information security standards prescribed by TAC 202 and to satisfy the requirements for a biennial compliance review of the information security program pursuant to Rule 202.76(c). The audit focused on determining compliance with the Texas Department of Information Resources (DIR) Security Standards Catalog, as required by TAC 202 rule §202.76(c).

Scope and Methodology

The scope of the audit included current information security controls in place at UTPB. We performed a risk assessment to identify high-risk areas within the TAC 202 provisions that were in effect at the time of our audit. Along with this, we considered the results from the prior audit along with the implementation status of recommendations. Audit procedures included interviews with management and staff; review of current policies, procedures, guidelines, and other supporting documentation; a self-assessment by the UTPB Chief Information Security Officer (CISO) regarding the status of DIR Security Standards Catalog implementation by UTPB; and limited testing of the controls determined by the CISO to be implemented.

Our audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

Ranking Criteria

All findings are ranked based on an assessment of risk factors, as well as the probability of a negative occurrence if the risk is not adequately mitigated. The criteria for the rankings are as follows:

Priority – An issue identified by an internal audit, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.

High - A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

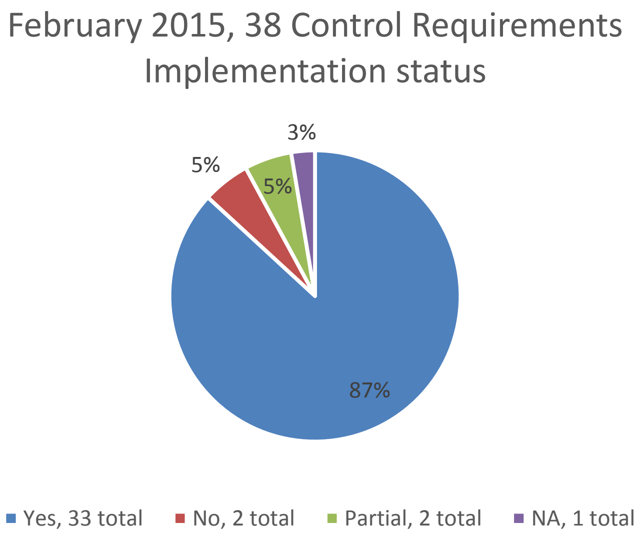
Medium – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level.

Low – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level.

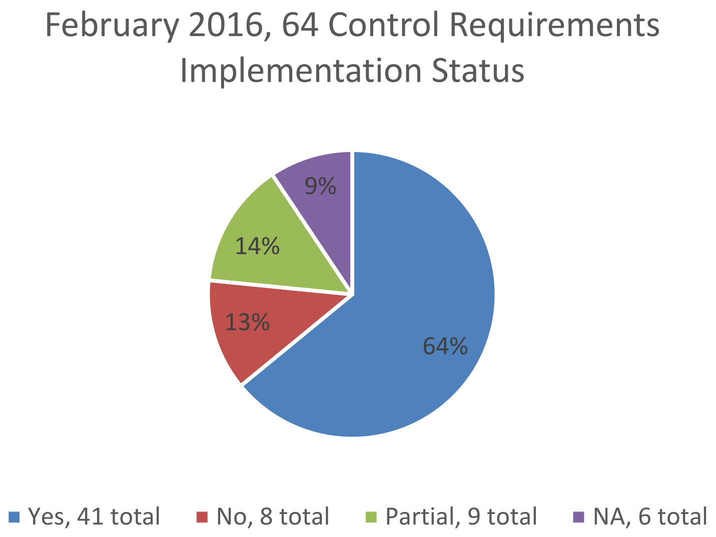
Audit Results

1. **<u>DIR Security Standards Catalog Self-Assessment</u>**
   UTPB is not in full compliance with the mandatory DIR Security Control Standards Catalog. Analysis of controls required by February 2015 indicated that 87% of the controls were in place. Additional analysis of controls required by February 2016 indicated that 64% of the controls were in place. These results are reflected by the implementation status in the charts listed below.

   For February 2015, 33 out of 38 control requirements (87%) had been fully implemented:



For February 2016, 41 out of 64 control requirements (64%) were fully implemented.



Assessed Level of Risk: High

Recommendation:
UTPB should implement steps to ensure full compliance with TAC 202, Rule §202.76, Security Control Standards Catalog. It should also be noted that there are additional control requirements that are required by February 2017.

Management Response:
We concur. UTPB shall work towards full compliance with the remaining control requirements that are applicable. There are some compliance requirements that are deemed to be an undue burden which will not be implemented as is permitted under TAC 202 as well as some that are not applicable (6) that will not be implemented.

Implementation Date:
August 31, 2017

Persons Responsible for Implementation:
Lowell Ballard, CIO
Steven Larizza, CISO

Status of Prior Year Findings and Recommendations

We followed up on four findings and recommendations from the previous TAC 202 (FY 2014) audit report. Management has implemented all of the recommendations from FY 2014. See ***Appendix A*** for detailed results.

Conclusion

Based on the audit procedures performed, UTPB is not in full compliance with TAC 202, Rule §202.76, Security Control Standards Catalog.

APPENDIX A

STATUS OF PRIOR YEAR FINDINGS AND RECOMMENDATIONS

No.	Finding	Recommendation	Status
1.	**<u>Management and Staff Responsibilities-§202.71</u>** TAC §202.71 (b) requires that institutions of higher education are responsible for defining all information classification categories. University of Texas System Policy UTS165 also requires data classification at the institution level. However, UTPB has not adopted and included data classification standards in its information technology (IT) operating procedures.	**Recommendation:** UTPB should review, update as necessary, and include data classification standards in its IT operating procedures. **Management Response (Original):** We concur. The University will develop the University's Information Security web pages to include the standards in its information technology procedures. This change will be communicated to the campus via email notification. **Anticipated Implementation Date (Original):** August 31, 2015 – Posted to the UTPB website. **New Implementation Date:** January 31, 2016	Implemented.
2.	**<u>Managing Security Risks-§202.72</u>** TAC §202.72 (a) requires that a risk assessment of information resources be performed and documented. It also requires that the risk assessment be updated based on inherent risk. IRD participates annually in providing information for the internal audit risk assessment process. However, this risk assessment process is of a different scope and uses different criteria in determining risk than the IT risk assessment process required by TAC 202.	**Recommendation:** IRD should complete IT security risk assessments as required under TAC 202 and include the Chief Information Security Officer (CISO) in the process. **Management's Response:** We concur. UT System has procured the necessary tools for Information Security to do risk assessments, called RSA Archer. **Anticipated Implementation Date**: A risk assessment of the Information Security Program will be completed by July 31, 2015. **New Implementation Date:** January	Implemented

No.	Finding	Recommendation	Status
		13, 2016	
3.	**Business Continuity Planning- §202.74** This section of the TAC requires that UTPB have a disaster recovery plan, obtain approval of the plan from the University head (or designee), and that the plan be tested annually. The University has a plan; however, approval of the plan by the University head (or designee) could not be documented. In addition, the plan should be updated to include current systems such as PeopleSoft. Finally, testing of the plan was not formally documented in detail.	**Recommendation**: The disaster recovery plan should be updated, approved by the University head (or designee), and annual testing documentation should be formally documented in detail with information to include items such as: exact steps taken; who performed the testing; the results of such testing, and management review and approval. **Management's Response:** We concur. UTPB IRD will review and update the existing disaster recovery plan and obtain appropriate management review and approvals. Once approved, the plan will be tested, documented in detail and reviewed by management. Due to the number of resources currently referenced that are in the process of migration and the current vacant CIO position, we plan to begin review immediately but will not be able to fully complete and test until those projects are completed. Barring any unforeseen circumstances, it is expected that this can be completed before the end of 2015; however there are a number of variables that could affect that date, so the implementation date takes that into account. **Anticipated Implementation Date:** March 31, 2016	Implemented
4.	**Information Resources Security Safeguards- §202.75** This section of the TAC requires that each institution of higher education head or designee and information security officer shall create, distribute, and implement	**Recommendation** UTPB should review, update as necessary, and include the Information Security Manual in its IT operating procedures. **Management's Response (Original):** We concur. The Information Security	Implemented

No.	Finding	Recommendation	Status
	information security policies. UTPB has information security policies and the CISO (Chief Information Security Officer) has developed a draft Information Security Manual which has not been adopted and included in its IT procedures.	Manual is under review by the CISO and will be ready to send to the VPBA in July 2015. **Anticipated Implementation Date (Original):** August 31, 2015 – Posted to the UTPB website. **New Implementation Date:** January 31, 2016	