March 26, 2018

Mr. Steven Larizza, Chief Information Security Officer
The University of Texas of the Permian Basin
4901 E. University Boulevard
Odessa, Texas 79762

Dear Mr. Larizza:

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 2018 Audit Plan and was conducted in accordance with guidelines set forth in UTS129, the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing,* and *Generally Accepted Government Auditing Standards* (GAGAS).

The objective of our audit was 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 S. Spencer

Glenn Spencer, CPA
Institutional Chief Audit Executive

cc: Dr. Sandra Woodley, President
Mr. Mark McGurk, CPA, Vice President for Business Affairs

The University of Texas
of the Permian Basin

FY 2018 TAC 202 – Audit Report

March 2018

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

Table of Contents

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 2018 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* and *Generally Accepted Government Auditing Standards* (GAGAS).

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* and the Generally Accepted Government Auditing Standards.

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.

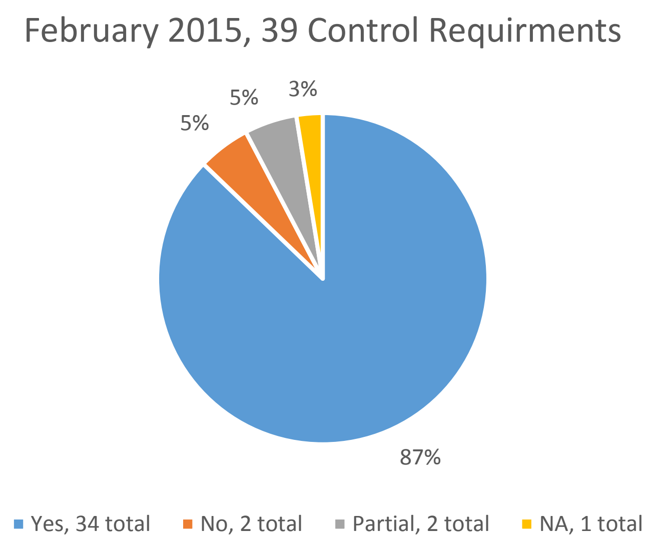
High - A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

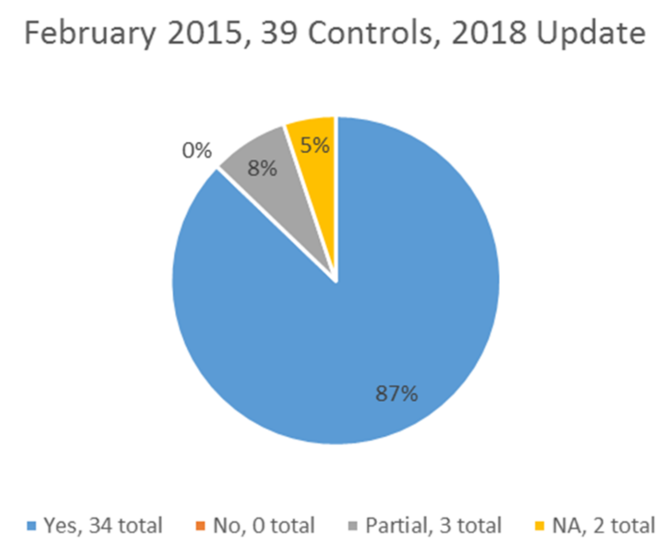
Medium – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level.

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.

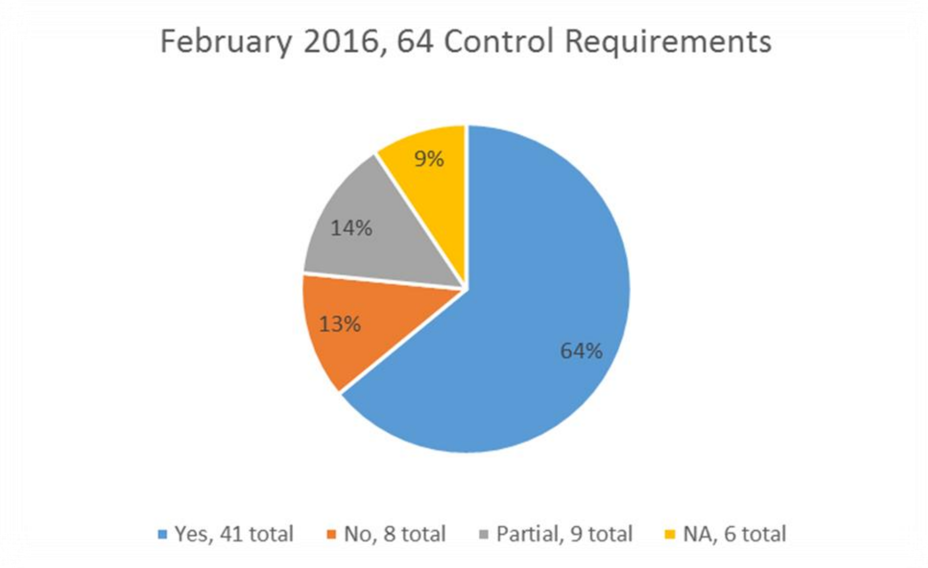
Audit Results

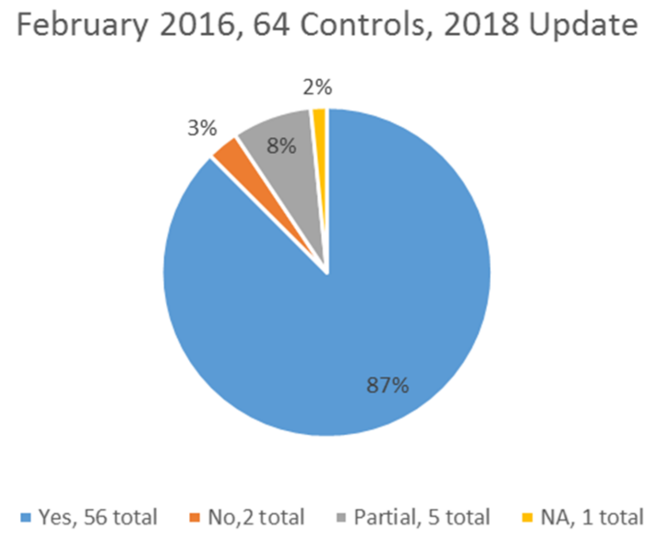
1. **DIR Security Standards Catalog Self-Assessment**
   UTPB is not in full compliance with the mandatory DIR Security Control Standards Catalog. An analysis of controls required by February 2015 completed in 2016 indicated that 87% of the controls were in place. An updated analysis completed in 2018 on these same controls required indicated that 87% of the controls were in place. The completion percentages for the February 2015 requirements are the same, however, there was movement from controls not implemented to partially implemented or not applicable. There were no February 2015 controls indicated as not being implemented. These results are reflected by the implementation status in the charts listed below.



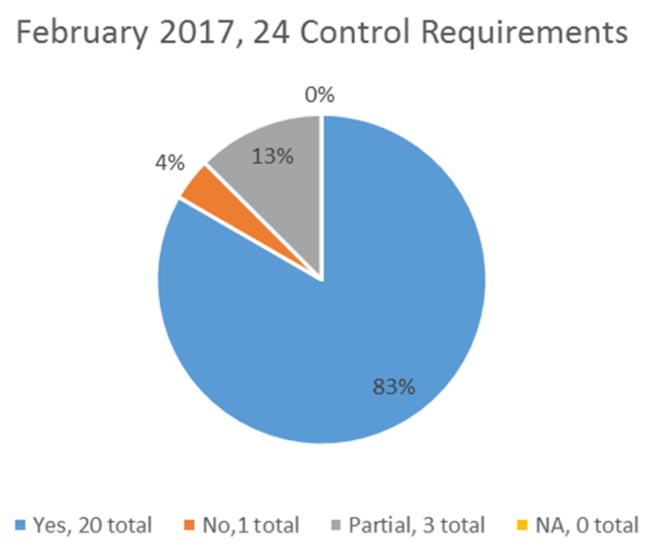


For February 2016, 41 out of 64 control requirements (64%) were fully implemented, as can be seen in the chart below. However, in the 2018 Audit, 87% of the controls were implemented. The total amount of controls not implemented to being implemented decreased from 8 to 2.

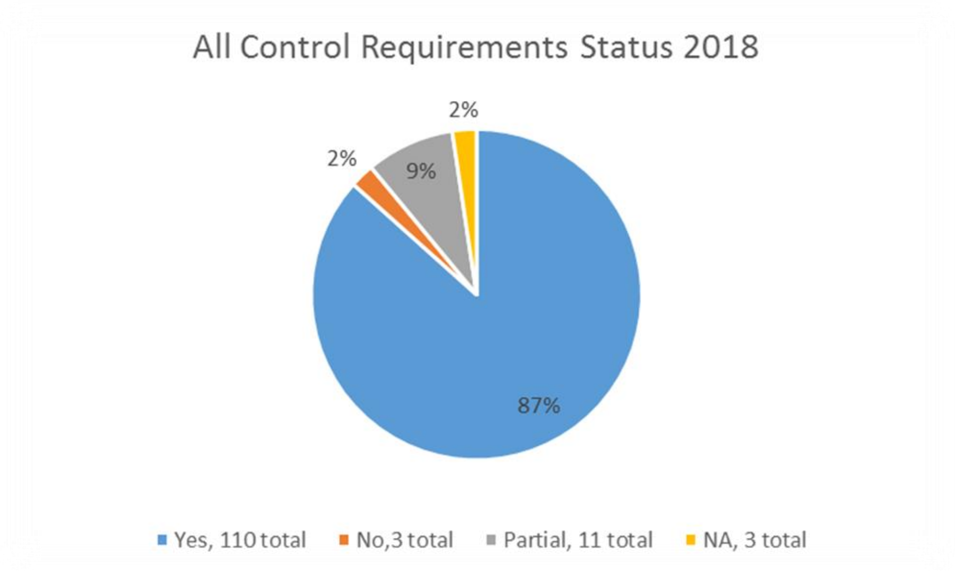

February 2016, 64 Control Requirements


February 2016, 64 Controls, 2018 Update

The following chart displays the controls required by February 2017, as found in the 2018 TAC 202 Audit.



The chart below is a combined representation of the status of all controls per the 2018 Audit. 87% of all controls are implemented. There are 110 controls implemented, 3 not implemented, 11 partially implemented, and 3 not applicable. Of the three controls not implanted, IR-2 deals with updating training for 2018 that employees receive regarding information security awareness, the second, PE-15, deals with water damage protection. There is a water pipe that was installed in the datacenter floor upon construction of the Science and Technology Building. No automatic shut-off was installed. The last control that was not implemented is RA-1, no risk assessment policies and procedures have been written for information systems. All three of the controls that were indicated as NA (not applicable) deal with applications developed within UTPB. The fact that UTPB does not develop in-house applications makes the three controls not applicable.



Assessed Level of Risk: High

<u>Recommendation</u>:
UTPB should implement steps to ensure full compliance with TAC 202, Rule §202.76, Security Control Standards Catalog and continue to document any controls for which the university is in a non-compliance status; any controls that the CISO determines are not applicable; and controls for which the university is in partial compliance.

According to TAC 202.71, *the Information Security Officer, with the approval of the state institution of higher education head, may issue exceptions to information security requirements or controls in this chapter. Any such exceptions shall be justified, documented, and communicated as part of the risk assessment process.* It is recommended that this action be taken if there are control requirements that meet the aforementioned criteria.

<u>Management Response</u>:
The CISO will create a document for the President's approval regarding the three controls that are considered "Not Applicable". The controls that are not implemented will be addressed with a plan for when they will be completed (also approved by the President as applicable). Controls that are partial will have a plan for their completion.

<u>Implementation Date</u>: September 30, 2018

<u>Persons Responsible for Implementation</u>:
Steven Larizza, CISO

Status of Prior Year Findings and Recommendations

We followed up on one finding and recommendation from the previous TAC 202 (FY 2016) audit report. Management has not fully implemented the recommendations from FY 2016. 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.	**1. DIR Security Standards Catalog Self-Assessment** 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.	**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.**	In progress. The finding is determined to not be closed out due to control requirements that are not in compliance and the proper approvals required in TAC 202 for controls that may be considered as exceptions for implementation were not received, justified or documented and

No.	Finding	Recommendation	Status
		Implementation Date: **August 31, 2017** **<u>Persons Responsible for Implementation</u>:** Steven Larizza, CISO	communicated as part of the risk assessment.