



Office of Internal Audit

December 14, 2020

Dr. Sandra Woodley, President
The University of Texas Permian Basin
4901 E. University Boulevard
Odessa, Texas 79762

Dear Dr. Woodley:

We have completed our TAC 202 System Security audit as included in the FY 2021 audit plan. We conducted our audit 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) as issued by the Comptroller General of the United States.

The purpose of our audit was to determine whether the UTPB information security program complies with the security standards prescribed by Texas Administrative Code (TAC 202), and to satisfy the requirements for a biennial compliance review of the information security program pursuant to Rule 202.76(c).

Based upon the results of our audit, it is our opinion that UT Permian Basin is in overall compliance with TAC 202.

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

Sincerely,

A handwritten signature in black ink that reads "Glenn S. Spencer".

Glenn Spencer, CPA, CGMA
Chief Audit Executive

cc: Cesario Valenzuela, CPA, CFO and Vice President for Business Affairs
Robert Belk, CISSP, Chief Information Security Officer

The University of Texas Permian Basin



TAC 202 – System Security Audit December 2020

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

Table of Contents

Executive Summary	3
Objective	3
Scope and Methodology	3
Risk Ranking Criteria	4
Audit Results	4
Prior Findings and Recommendations	4
Conclusion	4
Appendix A – Status of Prior Findings and Recommendations	5

Executive Summary

We have completed our audit of the UTPB information resources security program’s compliance 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).

Risk Level	Findings
	None

OVERALL
CONCLUSION

UT Permian Basin is in overall compliance with the requirements of Texas Administrative Code (TAC) 202.

Objective

The objective of our audit was to determine if the UTPB information resources security program complies with the information security requirements prescribed by TAC 202 and to satisfy the additional requirement for a biennial compliance review of the information security program pursuant to Rule 202.76(c).

Scope and Methodology

We reviewed each of the seven main sections of TAC 202 (202.70-202.76). The UTPB CISO (Chief Information Security Officer) was interviewed and requested to provide supporting documentation regarding compliance with each section of TAC 202. For Section 202.76, the CISO provided the status of UTPB’s compliance with NIST (National Institute of Standards and Technology) security control standards. Our audit included the following procedures:

- Gained an understanding of the TAC 202 requirements
- Interviewed UTPB CISO regarding TAC 202 compliance
- Reviewed supporting documentation for each TAC section and tested sample of security control standards

We conducted our audit in accordance with guidelines set forth in UTS 129; with the Institute of Internal Auditors’ *International Standards for the Professional Practice of Internal Auditing*; and with *Generally Accepted Government Auditing Standards (GAGAS)* as issued by the Comptroller General of the United States.

Risk Ranking Criteria

Risk Level	Definition
PRIORITY	An issue or condition, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of UT Permian Basin or UT System as a whole.
HIGH	Risk that is considered to be substantially undesirable and results in a medium to high probability of significant adverse effects to UT Permian Basin either as a whole or at the college/department/unit level.
MEDIUM	Risk that is considered undesirable and has a low to medium probability of adverse effects to UT Permian Basin either as a whole or at the college/department/unit level. Without appropriate controls, the risk will occur some of the time.
LOW	Considered to have minimal probability of adverse effects to the UT institution either as a whole or at the college/ school/unit level. Even with no controls, the exposure to UT Permian Basin will be minimal.

Audit Results

UTPB is in overall compliance with the requirements for each of the seven TAC 202 sections. Of the 127 required security standards contained in the security control standards catalog, 123 or 97% of the standards were either in place, partially in place, or not applicable to UTPB. For the four security standards that have not been met, these were not under the authority of the CISO, and were not material to the overall compliance of UTPB.

Status of Prior Findings and Recommendations

Management has implemented the sole recommendation from the prior year audit. See **Appendix A** for detailed results.

Conclusion

Based upon the results of our audit, it is our opinion that UT Permian Basin is in overall compliance with the requirements of Texas Administrative Code 202.

Appendix A

Status of Prior Findings and Recommendations

No.	Finding	Recommendation	Status
1.	<p>1. DIR Security Standards Catalog Self-Assessment</p> <p>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.</p> <p>Assessed Level of Risk: High</p>	<p><u>Recommendation:</u> 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</p> <p><u>Management Response:</u> 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.</p> <p>Implementation Date: August 31, 2017</p> <p><u>Persons Responsible for Implementation:</u> Steven Larizza, CISO</p>	<p>Implemented. Followed up on and closed out on 11-1-2018.</p>