Meeting of the Board of Regents

Audit Committee

November 10, 2022
Waco, Texas

TSTC
Texas State
Technical College ™

TABLE OF CONTENTS

Audit Committee
[Tony Abad (Chair), Kathy Stewart, Lizzy de la Garza Putegnat]

Minute Orders:

Proposed MO #

(c) denotes Consent Agenda Item

(c) denotes Consent Agenda Item

Board Meeting Date: November 10, 2022   **Proposed Minute Order #:** IA 02-22(c)

Proposed By: Jason D. Mallory, Director of Audits

Subject: Internal Audit Charter - Review and Reapproval

Background: The Texas Internal Auditing Act, Chapter 2102 of the Texas Government Code, requires all State agencies that have an operating budget that exceeds $10 million, has more than 100 full-time equivalent employees, or receives and processes more than $10 million in cash in a fiscal year have an internal audit function. Each internal audit function must be led by a person who is either a certified public accountant or certified internal auditor. The internal audit function shall also conform to the Standards for the Professional Practice of Internal Auditing, the Code of Ethics contained in the Professional Practices Framework as promulgated by the Institute of Internal Auditors, and generally accepted government auditing standards.

The Professional Practices Framework requires a charter be adopted by the governing board which defines the responsibilities and authority of the internal audit function. This charter must be reviewed periodically for changes. Traditionally, this review has been performed annually at the Fall meeting of the TSTC Board of Regents, with reapproval only occurring if changes are made. In fiscal year 2021, the Board of Regents directed the charter be reviewed and reapproved annually, irrespective of changes. This review and reapproval was last performed on November 11, 2021, at Minute Order #34-21(c).

Justification: This minute order is intended to satisfy the annual review and reauthorization requirement of the charter for fiscal year 2023.

The charter attached to this minute order differs from the one previously presented on November 11, 2021. The charter historically has been presented as a Statewide Operating Standard. As such, it was subject to formatting standards of those documents, and was approved by management.

It has been rewritten to be a stand-alone document, subject only to the review of the Audit Committee, and approval by the Board of Regents. The charter still defines the purpose, role, authority, reporting structure, and responsibilities of the Department of Audits.

Additional Information: None

Fiscal Implications: No significant fiscal impact.

Attestation: The Minute Order is in compliance with all applicable laws and regulations to the best of my knowledge.

Attachment(s):   Internal Audit Charter

Recommended Minute Order: "The Texas State Technical College Board of Regents approves the Internal Audit Charter which grants specific authority, responsibilities and limitations to the Internal Audit Department. All previous versions of this document in the form of SOS GA 1.4 are rescinded."

Recommended By:

Jason D. Mallory, Director of Audits

INTERNAL AUDIT CHARTER
for
Texas State Technical College

INTRODUCTION
Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

PURPOSE
The purpose of the Department of Audits at Texas State Technical College (TSTC) is to provide the Board of Regents an independent appraisal of the adequacy and the effectiveness of the College's system of internal controls as they relate to accounting, operating, and compliance objectives, and the quality of performance when compared with established standards. The primary objective is to assist the Board of Regents, Chancellor and management in the effective discharge of their responsibilities.

ROLE
The internal audit activity is formally established by Texas Government Code, Title 10, Subtitle C, Chapter 2102, otherwise known as the Texas Internal Auditing Act. The Department of Audits is the College's internal audit activity. The Audit Committee of the Board of Regents provides oversight. The Department of Audits works to be a trusted advisor to management in the areas of governance, risk management and internal controls.

PROFESSIONALISM
The Institute of Internal Auditors' mandatory guidance, which include the Definition of Internal Auditing, the Code of Ethics, the Core Principles, and International Standards for the Professional Practice of Internal Auditing (Standards), as well as Generally Accepted Government Auditing standards and the Texas Internal Auditing Act provide structure for the Department of Audits. This mandatory guidance constitutes principles for the fundamental requirements for the Professional Practice of Internal Auditing, and for evaluating the effectiveness of the Department of Audits' performance.

The Institute of Internal Auditors' Implementation Guidance and Supplemental Guidance will also be adhered to as applicable. In addition, the Department of Audits will adhere to relevant TSTC policies and procedures, as well as performance requirements set forth in a departmental maintained procedures manual.

AUTHORITY
The Department of Audits, with strict accountability for confidentiality and safeguarding records and information, is authorized unrestricted access to any and all TSTC records, both manual and electronic; physical properties and assets; activities; systems; and personnel pertinent to carrying

out any approved engagement. All TSTC employees should try in a timely and ethical manner to assist the Department of Audits in fulfilling its roles and responsibilities when requested for an audit, investigation, or other activity. The Chief Audit Executive (CAE) will also have free and unrestricted access to the Audit Committee.

ORGANIZATION

The Department of Audits is an integral part of TSTC and functions in accordance with the policies established by the Board of Regents. To provide for the independence of the Department of Audits, the CAE is appointed directly by the Board of Regents. The CAE reports functionally to the Board of Regents, but administratively to the Chancellor.

The CAE will communicate and interact directly with the Audit Committee during committee meetings, executive sessions where allowed by law, and between committee meetings, as appropriate and needed. Responsibilities of the Audit Committee are outlined in the Board of Regents' Bylaws.

INDEPENDENCE AND OBJECTIVITY

The Department of Audits will remain free from interference by any element in the College. No manager may interfere with, or have undue influence on, audit selection, scope, audit procedures and techniques, frequency, timing, or report content. This is intended to maintain a necessary independent and objective mental attitude.

Internal auditors will have no direct operational responsibility or authority over any activity outside of the Department of Audits. Accordingly, they will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair their judgment or ability to act without bias. Internal auditors may provide assurance services where they have previously performed consulting services provided the nature of the consulting did not impair objectivity, and provided individual objectivity is managed when assigning resources to the engagement.

Internal auditors will exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors will make a balanced assessment of all the relevant circumstances and not be unduly influenced by their own interests or by others in forming judgments.

The CAE will confirm to the Audit Committee at least annually the organizational independence of the Department of Audits and its staff members.

RESPONSIBILITY

The Department of Audits scope encompasses, but is not limited to, the examination and evaluation of the adequacy and effectiveness of the College's governance, risk management, and internal controls as well as the quality of performance in carrying out assigned responsibilities to achieve the College's stated goals and objectives. This includes:

- Developing a flexible, annual audit plan using an appropriate risk-based methodology, including any risks or control concerns identified by management, and submitting that plan to Audit Committee for review and to the Board of Regents for approval on an annual basis.

- Developing and utilizing a systematic, disciplined approach for performing internal audits.

- Providing audit coverage that consistently meets the needs and expectations of the Board of Regents, Chancellor, and oversight agencies where applicable.

- Developing relationships throughout the College to become a trusted advisor to management on risk management, governance and internal control matters.

- Maintaining a professional audit staff with sufficient knowledge, skills, abilities, experience, and professional certifications.

- Evaluating risk exposure relating to achievement of the College's strategic objectives.

- Evaluating the reliability and integrity of financial and operational information and the means used to identify, measure, classify, and report such information.

- Evaluating the systems established to ensure compliance with policies, plans, procedures, laws, and regulations which could have a significant impact on the College.

- Evaluating compliance with laws, regulations, policies, procedures, and controls.

- Evaluating the means of safeguarding assets and, as appropriate, verifying the existence of such assets.

- Evaluating the effectiveness and efficiency with which resources are employed.

- Evaluating operations or programs to ascertain whether results are consistent with established objectives and goals and whether the operations or programs are being carried out as planned and the effectiveness and efficiency of the operations and programs.

- Evaluating risk management, control, and governance processes.

- Coordinating with external auditors and serving as a liaison, as applicable.

- Performing consulting services related to governance, risk management and control as appropriate, and documenting the understanding of the consulting engagement objectives, scope, responsibilities and expectations for significant engagements.

- Performing advisory services related to governance, risk management and control, as appropriate. Such services may include management requests, participation on College committees, policy reviews, and participation on teams for information technology projects and business process improvements.

- Evaluating specific operations at the request of the Audit Committee or management, as appropriate.

- Conducting inquiries or investigations of suspected fraudulent activities in accordance with SOS GA 1.15, Fraudulent Use of Assets and Resources.

- Assisting with the anti-fraud program for the College by implementing an anonymous fraud hotline per SOS GA 1.17, Fraud Hotline.

- Facilitating risk assessment processes with management.

- Maintaining a list of management corrective action plans from audits and projects, and performing follow-up audits on those plans as necessary.

- Providing a systematic, disciplined approach to evaluate and improve the effectiveness of the Colleges risk management, control, and governance processes related to contracts and risk-based testing of contract administration as required by Texas Education Code, Section 51.9337(h).

- Presenting educational opportunities periodically to the Audit Committee on the subject of internal auditing and risk management.

- Staying abreast of current risk, regulatory, and audit trends, and communicating those to management and the Audit Committee, as appropriate.

INTERNAL AUDIT PLAN

At least annually, the CAE will submit to the Board of Regents an internal audit plan for review and approval. The internal audit plan will consist of a work schedule as well as budget and resource requirements for the next fiscal year. The internal audit plan will be developed based on a prioritization of the audit universe using an appropriate risk-based methodology, including input of Executive and Senior managers, and the Board of Regents. The CAE will consider audits, at a minimum, of information security, contracts, contract administration, investments, and other areas. The CAE will review and adjust the plan, as necessary, in response to changes in the internal audit resource levels or those of the College's business, risks, operations, programs, systems, and controls. Any significant deviation from the internal audit plan will be communicated to the Audit Committee and approved by the Board of Regents.

REPORTING AND MONITORING

The CAE will communicate the results of each internal audit engagement to the appropriate managers in the form of a written report. Internal audit results will also be communicated to the Audit Committee and state and federal oversight agencies as required.

Communication of results of each engagement may vary in form and content depending upon the nature of the engagement and the needs of the client. Where applicable, a formal internal audit report will include management's response and corrective action taken or to be taken in regard to

the specific findings and recommendations. Management's response should include a responsible person and implementation date for all anticipated corrective action plans.

The Department of Audits will follow-up on management corrective action plans to address engagement findings and recommendations, and will report the results to appropriate management members and the Audit Committee. All significant findings will remain as open issues until reviewed and cleared by the Department of Audits.

The Department of Audits will fulfill reporting requirements for audit reports and the annual report, including the annual audit plan, as prescribed by the Texas Internal Auditing Act.

The CAE will periodically report to the Audit Committee on the Department of Audits purpose, authority, and responsibility, as well as performance relative to its audit plan. Reporting will also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by the Audit Committee.

QUALITY ASSURANCE AND IMPROVEMENT PROGRAM

The CAE will maintain a quality assurance and improvement program that covers all aspects of the internal audit activity. The program will include an evaluation of the internal audit activity's conformance with the Definition of Internal Auditing, the Core Principles, and the Standards. The program also assesses the efficiency and effectiveness of the Department of Audits and identifies opportunities for improvement.

The CAE will communicate to the Audit Committee the Department of Audits quality assurance and improvement program, including results of ongoing internal assessments and external assessments conducted at least every three years.

RELEVANT STATUTES AND POLICIES
- Texas Internal Auditing Act
- Applicable College Statewide Operating Standards Regulations
- SOS GA 1.14, Audits and Reviews by External Auditors
- SOS GA 1.15, Fraudulent Use of Assets and Resources
- SOS GA 1.16, Reporting of Wrongdoing or Retaliation
- SOS GA 1.17, Fraud Hotline
- Texas Education Code, Section 51.9337(h)

APPROVAL

The Internal Audit Charter was last submitted by the CAE for review by the Audit Committee and approval by the Board of Regents on November 11, 2021 at Minute Order #34-21(c).

INTERNAL AUDITS

Description	Division/Campus	Status	Project No.	Report Date	Last Audit Date	Audit Reason
Public Funds Investment Act Audit	Finance	Complete	22-003A	9/24/21	9/26/19	Required every 2 years
Virtual Private Network Audit (TAC 202)	OIT	Complete	22-004A	11/22/21	-	Risk Based
Benefits Proportionality Audit	Payroll	Complete	22-008A	12/8/21	12/6/19	Required every 2 years
Academic Records Management Audit	Registrar/Instructional	Complete	22-005A	12/17/21	-	Risk Based
Coronavirus Aid, Relief, and Economic Security (CARES) Act Compliance Audit	OSP/Financial Aid/Student Services	Complete	22-006A	12/20/21	7/6/21	Risk Based
Internal Network Penetration Test	Fort Bend Campus	Complete	22-012A	1/4/22	3/29/19	Risk Based
Tuition Audit	Finance	Complete	22-015A	3/29/22	7/8/14	Risk Based
Audit of TWC Server	Business Analysis	Complete	22-022A	5/16/22	-	Risk Based
Canvas System Audit (TAC 202)	Instructional/IT	Complete	22-021A	5/20/22	-	Risk Based
On-Line Learning Audit	Instructional	Complete	22-002A	6/6/22	-	Risk Based
TEC 51.9337 (Contracting) Audit	Contract Office	Complete	22-028A	6/8/22	9/23/21	Required Annually
Internal Network Penetration Test	North Texas Campus	Complete	22-031A	6/9/22	2/13/19	Risk Based
Police Evidence Room Inspections	Police	Partially Complete	22-018A	12/15/2021, 5/17/2022	Fiscal Year 2019	Risk Based
Cash Counts	Various	Partially Complete	22-017A	3/15/2022, 6/6/2022, 6/7/22, 6/10/22, 6/23/22	Fiscal Year 2013	Risk Based
TAC 202 Follow-up Audit	OIT	Complete	22-009A	6/30/22	5/12/22	Required Bi-annually
Bookstore Audit	Marshall Campus	Complete	22-034A	9/26/22	7/3/08	Risk Based

EXTERNAL AUDITS

Description	Division/Campus	Status	Project No.	Report Date	Last Audit Date	Audit Reason
Benefit Pay Replacement Desk Audit performed by the Comptroller's Office	Statewide	Complete	001-21-01	9/1/21		
Summary - State of Texas Federal Portion of the Statewide Single Audit Report for the Year Ended August 31, 2021 by the State Auditor's Office	Finance	Complete	22-320	2/28/22		
Summary - State of Texas Financial Portion of the Statewide Single Audit Report for the Year Ended August 31, 2021 by the State Auditor's Office	Finance	Complete	22-555	2/28/22		
A Summary Report on Full-time Equivalent State Employees for Fiscal Year 2021 by the State Auditor's Office	HR	Complete	22-703	3/31/22		
Audit of Compliance with the Public Funds Investment Act performed by the State Auditor's Office	Finance	Complete	22-034	6/30/22		
AY 2021 Single Audit Evaluation Management Letter for GEER Upskill & Reskill, Perkins Formula, Perkins Leadership 2-Yr by THECB	Office Sponsored Programs	Complete		8/10/22		

AY 2021 Single Audit Evaluation Management Letter for GEER TEOG Community Colleges, GEER TEOG , GEER New & Continuing Students by THECB	Office Sponsored Programs	Complete		8/10/22
Dual/Multiple Employment Desk Audit performed by the Comptroller's Office	Statewide	In progress - waiting on report		

OTHER INTERNAL PROJECTS

SAO Hotline: Received a complaint of employee related issues within a department. Results: The complaint was forwarded to HR for resolution. They concluded that recent organizational changes were not well communicated. One manager was terminated. For future changes that will result in changes to job titles, a matrix will be required that documents decision rationale.	Enrollment Services	Complete	22-010I	12/15/21
SAO Hotline: Received a complaint of a perceived race bias which has allegedly resulted in some employees not being required to submit leave requests. Results: The complaint was forwarded to HR for resolution. They reviewed the leave requests and use of select employees within OIT. They determined leave requests were being submitted, as required. No trends or anomalies were identified that supported the allegation.	OIT	Complete	22-013I	12/15/21
Internal Audit consulted with management of the Dental Hygiene Program regarding how to better control fees charged/collected during patient visits.	Dental Hygiene Program	Complete	22-023P	2/2/22
Internal Hotline: On 12/11/21, an anonymous concern was reported from presumably an instructor. The concern centered around the detrimental impact students repeatedly registering for courses to receive financial aid and then dropping courses will have on individual performance evaluations. Results: The concern was discussed with Instructional management, who indicated that student persistency and success will be elements of future performance evaluations, but will be refined as appropriate. There is no evidence of fraud, waste or abuse to investigate.	Instructional/Student Services	Complete	22-020I	2/2/22
Internal Hotline: On 1/19/22, an anonymous concern was reported related to alleged past criminal history of a current student, and the possibility he was an ongoing threat to other students. This report was immediately forwarded to the TSTC Police, Student Discipline, and Title IX personnel for follow-up and action. Results: The Police and Student Discipline took appropriate steps to mitigate the risk.	Instructional/Student Services	Complete	22-024I	2/3/22

Internal Hotline: On 1/27/22, an anonymous concern was reported related to employee fatigue of being a COVID Contract Tracer. Results: HR determined that most contact tracers received one-time bonuses in October 2021 based on their volume of work. All employees also received raises that same month connected with their permanent jobs. Finally, consideration is being given to another bonus as a result of the spiked activity that occurred in January.	HR	Complete	22-025I	3/15/22
Report by Management: On 2/15/22, an employee in student accounting reported a concern about fees being collected by the Dental Hygiene program. Specifically, the concern was that an employee was depositing student fees into her personal checking account. Results: Found no fraud or waste, but recommended that all payments by students be made directly to the cashier's office rather than to the program's lab assistant.	Dental Hygiene Program	Complete	22-027I	3/24/22
Internal Hotline: On 2/22/22, an anonymous concern was reported stating that a supervisor who is working remotely is difficult to contact. This reportedly impacted a student. Results: Forward to leadership in Student Enrollment to address. On 3/30/22, we were informed that the supervisor had evidence that she attempted several times to contact the student to demonstrate she was available and attempted to resolve the student's. Specific complaint appears to be a misunderstanding.	Student Rights - Abilene Campus	Complete	22-030I	3/30/22
Report by management: On 12/8/21, management notified us of a payment made to a fraudster based on fraudulent payment instructions. Results: Internal Audit has completed its investigation. The Police are currently performing a criminal investigation to identify the perpetrator. The College was able to recover all but $7,737.48 of the $87,400 that was originally wired.	A/P	Complete	22-019I	6/3/22
Concern brought by employees: Employee posted racist meme on his personal facebook account. At the time, his account listed his association with the College. Results: IA forwarded the concern to HR and Legal for review and action. The employee removed TSTC from his personal account, and was counseled about the matter by HR and the Provost.	Instructional	Complete	22-038I	8/1/22

Internal Hotline: 7/11/22, an anonymous concern was reported the hiring of a new manager, alleging unfair hring practices. Results: Forward to HR. On 8/2/22, HR concluded that the open position was posted for internal and external candidates. The external candidate that was hired was well justified based on her qualifications.	Enrollment Services	Complete	22-036I	8/2/22
Manager brought forward an elaborate reimbursement scam in which students applied for a fraudulent job listing that was forwarded to them by Career Services. The scam attempted to have students pay for equipment they needed. Results: No financial losses to students. The College paid for ID and Credit monitoring services for the 3 students who applied to the fraudulent job.	Career Services	Complete	22-039I	9/1/22
Audit of Foundation Controls (Limited Scope)	Foundation	Complete	22-037A	9/9/22
External Penetration Test Follow-up Audit	OIT	Complete	22-001A	9/21/22

Glossary	
A/P	Accounts Payable
HR	Human Resources
IA	Internal Audit
IT	Information Technology
OIT	Office of Information Technology
SAO	State Auditor's Office
TEC	Texas Education Code
TAC	Texas Administrative Code
TWC	Texas Workforce Commission

INTERNAL AUDITS

Description	Division/Campus	Status	Project No.	Report Date	Last Audit Date	Audit Reason
Internal Network Penetration Test	OIT/Harlingen Campus	Complete	23-004A	9/30/22	12/13/19	Risk Based
Personal Property Verification Audit	Finance/College-wide	In Progress	23-03A	10/3/22	-	Risk Based
TAC 202 Follow-up Audit	OIT	In Progress	22-009A	11/10/22	6/30/22	Required Bi-annually
American Rescue Plan Act – Higher Education Emergency Relief Fund III	Office of Sponsored Programs, Student Services	In Progress			12/20/21	Risk Based
Sick Leave Administration	HR	In Progress			-	Risk Based
TEC 51.9337 (Contracting) Audit	Contract Office				6/8/22	Required Annually
Payroll and Benefits Proportionality	Payroll				12/9/21	Risk Based
Internal Network Penetration Test	OIT/East Williamson County Campus				9/27/19	Risk Based
Internal Network Penetration Test	OIT/Waco Campus				3/10/20	Risk Based
Audit of General IT Controls	OIT				6/28/17	Risk Based
T-Drive Audit	OIT/Several Departments				-	Risk Based
Construction Audits	Construction				7/20/22	Risk Based
Audit of Remote Work Processes and Procedures	College-wide				-	Risk Based
Accounts Payable Audit	Finance				5/17/19	Risk Based
Audit within the Waco Physical Plant	Physical Plant				-	Risk Based
Audit within the Harlingen Physical Plant	Physical Plant				-	Risk Based

EXTERNAL AUDITS

OTHER INTERNAL PROJECTS

Description	Division/Campus	Status	Project No.	Report Date	Last Audit Date	Audit Reason
Internal Hotline: On 9/1/22, an anonymous concern was reported that employees were not being paid for flex time, and were being required to work long hours. Results: The concern was forwarded to HR. HR concluded that management attempted to provide appropriate work/life balance during the busy time, lunches and breaks were available, and pay was paid as appropriate.	Enrollment Services	Complete	23-006I	9/16/22		
Internal Hotline: On 10/4/22, an anonymous concern was reported from presumably an instructor. Allegedly, behavior concerns have been reported through Maxient on a particular student, but timely/appropriate action has not been taken. This lack of action has created a poor working environment. Results: Pending investigation.		Pending Review	23-010I			

	Glossary
A/P	Accounts Payable
HR	Human Resources
IA	Internal Audit
IT	Information Technology
OIT	Office of Information Technology
SAO	State Auditor's Office
TEC	Texas Education Code
TAC	Texas Administrative Code
TWC	Texas Workforce Commission

Texas State Technical College
Internal Audit
Summary of Audit Reports

Report Name & No.		Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
Audit of Foundation Controls (Limited Scope) (22-037A)	1.		No findings identified.			
External Penetration Tests - Follow-up Audit (22-001A)	1.		All recommendations implemented.			
Bookstore Audit (22-034A)	1.		No findings identified.			
Internal Network Penetration Test (23-004A) - Harlingen	1.	There needs to be a heightened awareness of cybersecurity risks College-wide. We were able to compromise 20% of the employees we tested through our enhanced social engineering tests.	12 of 61 people who were tested in 4 social engineering tests provided sensitive information inappropriately.	1.1 With assistance from Creative Services, implement an awareness campaign of cyber risks that reinforces training and expectations.	Larry McKee	10/31/22
Quarterly Results of Personal Property Verification Audit (23-003A)	1.		790 of 8,101 sample of assets verified as 10/5/22.			

Report Name & No.		Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
TAC 202 Compliance – Quarterly Update (23-002A)	1.		9 more controls were identified as being implemented.			
Career Services – Phishing Scam (22-039I)	1.	Staff was tricked into forwarding a fraudulent job posting to several students.	A phishing email publicizing a fake job opportunity was forwarded to over 600 students. Three applied.	1.1 One employee is designated as the primary contact and approver of all the jobs that come through hireTSTC or through email requests to post jobs. This employee will be responsible for ensuring the legitimacy of all requests before they are made available to students.	Kacey Darnell	8/1/22
				1.2 Provide specific cybersecurity training to employees.	Kacey Darnell	8/1/22
				1.3 Enhance email system settings to better identify questionable emails.	Larry McKee	8/1/22
Texas State Technical College System AY 2021 Evaluation Management Letter performed by THECB	1.		No findings identified.			

Report Name & No.		Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp.Sr Mgr	Expect. Complete Date
Texas State Technical College Waco AY 2021 Evaluation Management Letter performed by THECB	1.		No findings identified.			

Texas State Technical College
Internal Audit
Follow Up Schedule & Status

	Completion Summary		Audits cleared from (Added to) Schedule
	6/30/22	**9/30/22**	
Audits from FY 2017 & Earlier	3	3	0
Audits from FY 2018	1	1	0
Audits from FY 2020	1	1	0
Audits from FY 2021	3	2	1
Audits from FY 2022	8	6	2
Audits from FY 2023	0	1	(1)
Net Total	16	13	2

Highlights:

TAC 202 Audits: 9 more control was implemented.
Academic Records Management Audit (22-005A): One more corrective actions was implemented.
Annual Contract Audit (22-028A): All corrective actions were taken.
Personal Property Follow-up is underway. Results are encouraging as they relate to existence, training, monitoring.
Payment Fraud Investigation (22-019I): All corrective actions were taken.

A-17

Report Name & No., Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
Summary of Departmental Audits (Marshall Welding Department 17-013A, Fort Bend Diesel 17-023A, Fort Bend HVAC 17-022A), C. Wooten, Boykin	1. We identified numerous exceptions related to inventory control in the Welding Department. In 2021, the SAO also cited the following issues: The College's process was not adequate to ensure that donated assets were added to its inventory and SPA; the College's process was not adequate to ensure that it accounted for auctioned and disposed assets; the College does not perform a reconciliation between its financial record system and SPA for all assets; Law enforcement is not always notified within 48 hours of the College determining that an asset has been stolen; The College did not consistently determine employee negligence when investigating stolen assets.	1.1 SPA will no longer be used after 8/31/21, therefore, no reconciliation will be necessary. 1.2 Implement enhance fixed asset training that includes awareness to report donated assets. 1.3 Implementation of Workday 1.4 Utilize a cross divisional committee to review negligence related to stolen assets.	**Partially Complete:** 1.1 SPA is no longer used as of 9/30/2021; 1.2 Training has been developed Our results indicate 97% of employees successfully completed it. 1.3 Workday was implemented in April 2022, with all fixed assets being loaded an assigned to their respective stewards. Each steward can easily see what assets are assigned to them. 1.4. The CIAG Committee meets periodically to discuss missing assets, the reasons, and to decide steps for accountability. Audit 23-003A is underway to verify over 8,000 assets.		1.1 Complete, 1.2 Complete, 1.3 Complete, 1.4 Ongoing
TAC §202 Compliance Audits 22-004A,22-021A, 22-022A, McKee, Scherwitz	1. Several required controls were not yet implemented.	As noted in the report, a majority of the required controls have been implemented with the remaining controls being evaluated and addressed. For the controls not yet implemented, we are evaluating the associated risk to TSTC and associated applicability in our environment to prioritize implementation. IT Security along with TAC 202 compliance is a priority for TSTC.	**Ongoing:** At 10/5/22, 11 systems and the IT general controls have been audited. A total of 0 general controls and 6 (total for all systems audited) application controls were not yet implemented. In this quarter, 9 controls were improved to implemented status.		Ongoing

Report Name & No., Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
PCI Compliance Audit (18-009A), **Herrera**	1. Numerous IT related controls and/or their control elements, as prescribed by PCI DSS, have not been implemented. As such, PCI DSS compliance is not being fully met.	1.1 In an effort to ensure the protection of payment card data for students and employees, The Office of Information Technology has been working with Food Services to resolve a number of important control deficiencies during the audit and will continue to review and implement recommendations moving forward. As we anticipate that the review and implementation review of 100 controls across 6 objectives will take over a year, we will prioritize controls that have the largest impact on the protection of cardholder data. As part of this process, we will also implement the recommendation of an annual assessment of PCI-DSS controls to ensure ongoing adherence to PCI-DSS compliance changes.	**Ongoing:** At 7/5/22, only 37 controls were still in the process of being implemented for the Waco and Harlingen Cafeterias. In FY 2024, PCI will be re-audited to verify compliance to the new standards. Recommend no further audit work will be performed until that audit commences.		Ongoing

Report Name & No, Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
Airport Operations Audit (20-008A), Herrera, Semien	1. Contract management procedures should be enhanced to ensure all contract provisions are met.	1.3 Use of Taxiway: L3 was made aware of the need for them to halt using the taxiway and begin to remove their equipment. We will establish a timeline for them to remove the equipment in coordination with L3. Kevin Semien will be responsible for this task and timeline will be complete no later September 30, 2020.	**Pending Review:** At 6/21/22, the Airport was working on a new lease with L3 for 20 additional acres that would include the boneyard area. This was originally expected to be presented to BOR at their May 2022 meeting for review and approval. However, it was not ready in time. Airport Management is working on the MO to be presented at the August BOR meeting. Also, FAA/TxDot review and approval process has been initiated for the L3 Hanger Project that would occupy this area.		~~12/30/2020,~~ 8/31/22
Audit of Disbursements from Student Club Accounts (21-007A), Stuart-Carruthers, C. Wooten	1. Controls are not consistently applied to ensure disbursements from Club Accounts are authorized and appropriate.	1.1 The College will cease the practice of administering club accounts by Fall of 2021 as clubs transition their funds. Student Life and Student Accounting staff will encourage student clubs to house their student club funds in a bank account off campus that is opened specifically and exclusively for the registered and recognized TSTC club. The new bank accounts will be 100% legally owned and controlled by the clubs themselves (not TSTC), and the club funds will no longer be accounted for in TSTC systems.	**Ongoing:** On 10/4/22, determined there were 141 accounts valued at $90K still on the books. Accounting will research and close after year end.		12/31/22

Report Name & No., Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
Faculty Credentials Audit (21-018A), DeLeon	1. While the system of controls for faculty credentialing have been appropriately designed, full implementation is still ongoing.	1.2 Implement the Strategic Planning Online system.	**Pending Review:** 9/1/22. All current instructors have been input into the SPOL system and all supporting documentation has been uploaded to the system. This should clear pending testing of the SPOL system by IA.		~~12/31/2021,~~ 7/31/2022
		1.3 Finish self-audits of all instructors hired before 3/1/2020.	**Pending Review:** See above notes.		~~5/31/2022,~~ 7/31/2022
Academic Records Management Audit (22-005A), Stuart-Carruthers, Bowers, Yanez, Scherwitz, McKee	1. There are specific opportunities to better control the integrity of final grades recorded in Colleague. These opportunities include more closely monitoring and restricting access to the systems relied upon, considering implementation of a single standardized method for submitting final grades, and enhancing select controls for final grade change requests.	1.2 Over the next few years, each instructional department will be transitioning to a new learning management system. Once all departments have completed the transition, the new LMS will be TSTC's single method for maintaining gradebooks and posting grade.	**Ongoing:** Departments are now using Canvas. We will revisit this in December 2022.		12/31/23
Tuition Audit (22-015A), C. Wooten	1. A formal change management process should be established to ensure only approved rates and tiers are updated in Colleague, and to ensure Colleague performs its calculations as intended. We found over $46 thousand in undercharges that may have been prevented/more readily identified had such a change management process been implemented.	1.1 A change management plan will be implemented to segregate duties during the process of rate table changes and to ensure a reasonable amount of testing is undertaken before use in production. All rate table changes and program tier changes (which usually occur no more than once per year) after plan implementation should be overseen by the new change management plan.	**Pending Review**		9/1/22

Report Name & No, Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
Audit of Online Learning (22-002A), Cano-Monreal	1. A defined set of training expectations for instructors would enhance the likelihood that Online and Hybrid courses meet TSTC's desired quality standards. Currently, there is no formulated set of required training(s).	1.1 SOS ES 2.20 is currently under revision and review in the College's SOS Management system to be finalized by August 2022. The updated statement regarding training standards will read that completion of training is encouraged, rather than required. The Online Learning Department works with TSTC's Learning and Development Office to provide training every Friday focused on online instruction best practices. Training sessions are recorded and housed in the College's learning management system for faculty to view and complete an activity for credit, if they cannot attend a live session. Attendance at a session (verified by signing in at the event) or completion of the activity at the end of the recorded version are used to track faculty training completion.	**Pending Review**		8/31/22
Career Services – Phishing Scam), Darnell	1. Staff was tricked into forwarding a fraudulent job posting to several students.	1.1 One employee is designated as the primary contact and approver of all the jobs that come through hireTSTC or through email requests to post jobs. This employee will be responsible for ensuring the legitimacy of all requests before they are made available to students.	**Completed during audit.** Internal Audit will test understanding through social engineering attacks.		8/1/22

Report Name & No, Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
		1.2 Provide specific cybersecurity training to employees.	**Completed during audit.** Internal Audit will test understanding through social engineering attacks.		8/1/22
		1.3 Enhance email system settings to better identify questionable emails.	**Completed during audit.** Internal Audit will test understanding through social engineering attacks.		8/1/22

Report Name & No, Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
Internal Network Penetration Test (23-004A), McKee	1. There needs to be a heightened awareness of cybersecurity risks College-wide. We were able to compromise 20% of the employees we tested through our enhanced social engineering tests.	1.1 Engage C&CS to implement an awareness campaign.	Ongoing		10/31/22

A-23

TEXAS STATE TECHNICAL COLLEGE

Internal Audit Annual Report
Fiscal Year 2022

Prepared by
Jason D. Mallory, Director of Audits

Table of Contents   Section

I. Compliance with TGC, Section §2102.015: Posting the Internal Audit Plan, Internal Audit Annual Report, and Other Audit Information on the TSTC Website

TGC, Section §2102.015 requires the College to post certain information on its website. Specifically, the College must post the current year audit plan within 30 days of approval by the Board of Regents, and the following information to its website:

- The annual audit report for the previous fiscal year.
- A detailed summary of the weaknesses, deficiencies, wrongdoings, or other concerns raised by the audit plan or annual report.
- A summary of the action taken by the College to address concerns raised by the audit plan or annual report.

To comply with the requirements, TSTC Internal Audit will submit its Internal Audit Annual Report to the College's website coordinators to be posted on the Internal Audit section of the College's website no later than 30 days after the TSTC Board of Regents approves the current year audit plan at its August meeting. This Annual Report includes the approved fiscal year 2023 audit plan. Furthermore, all Internal Audit reports are posted in the Board of Regents section of the TSTC website under the meeting agendas section. These are posted within 30 days after each meeting of the Board of Regents. These reports include detailed summaries of the weaknesses, deficiencies, wrongdoings, or other concerns found during each audit, if any, as well as summaries of the actions taken by the College to address those concerns. Information is available as far back as August 2015.

II. Internal Audit Plan for FY 2022

The Board of Regents approved the original internal audit plan for FY 2022 on August 19, 2021, with Minute Order #24-21(c). There were no deviations from the original internal audit plan, but the audit for the bookstore on the Marshall campus was still in progress at 8/31/22.

Texas Government Code §2102.005(b) requires a state agency to consider methods for ensuring compliance with contract processes and controls and for monitoring agency contracts. To comply with this provision, an internal audit of contract compliance is conducted annually. In FY 2022, an audit related to grounds maintenance contracts was performed. This is listed below as Report # 22-028A that was completed on June 8, 2022. We identified minor billing, and opportunities to improve monitoring of background check and insurance requirements.

An audit of benefits proportionality was conducted in FY 2022 to address the benefits proportionality audit requirement prescribed in Rider 8, page III-50, of the General Appropriations Act of the 87th Legislature. Represented below as Report # 22-008A dated December 9, 2021, one finding was identified in which $67,984.46 in disallowed benefits were paid from appropriated funds. That amount was refunded to the Comptroller's Office on November 8, 2021. For fiscal year 2023, another audit will be conducted on benefits proportionality.

Fiscal Year 2022 Internal Audit Plan

Project Description	Division/Campus	Report Number	Report Date	Status
TEC 51.9337 Contracting Audit	Procurement	22-028A	6/8/22	Complete
Public Funds Investment Act Audit	Finance	22-003A	9/24/21	Complete
Benefits Proportionality Audit	Finance, Payroll	22-008A	12/9/21	Complete
Coronavirus Aid, Relief, and Economic Security (CARES) Act Compliance Audit	Finance, OSP, Financial Aid	22-006A	12/20/21	Complete
Internal Network Penetration Test	North Texas campus	22-031A	6/9/22	Complete
Internal Network Penetration Test	Fort Bend campus	22-012A	1/4/22	Complete
Tuition Audit	Finance	22-015A	3/29/22	Complete
Bookstore Audit	Marshall Campus			In Progress
On-Line Learning Integrated Audit	OIT, Instruction	22-021A, 22-002A	5/20/22, 6/6/22	Complete

Surprise Cash Counts	Various departments, All campuses	22-017A	3/15/22, 6/6/22, 6/7/22, 6/10/22, 6/23/22	Complete
Surprise Police Evidence Room Inspections	Campus Police Departments	22-018A	12/15/21, 5/17/22	Complete
Virtual Private Network Audit	OIT	22-004A	11/22/21	Complete
Audit of the TWC Server	Business Intelligence, OIT	22-022A	5/16/22	Complete
Academic Records Management Audit	Instruction, Registrar	22-005A	12/17/21	Complete
TAC 202 Follow-up	OIT	22-009A	10/7/21, 3/10/22, 5/12/22, 6/30/22	Complete

Two FY 2021 audits were also completed in FY 2022. Those included the TEC 51.9337 Contracting Audit (report #21-028A), and an Accounts Receivable Billing Audit (report #21-003A).

Reports for all completed audits listed above are posted in the Board of Regents section of the TSTC website under the meeting agendas section at https://www.tstc.edu/about/board-of-regents. Each report contains detailed summaries of the weaknesses, deficiencies, wrongdoings, or other concerns found during each audit, if any, as well as summaries of the actions taken by the College to address those concerns.

III. List of Consulting Engagements and Non-audit Services Completed in FY 2022

The following schedule summarizes projects, other than planned audits, that were completed or nearing completion.

Report #	Date	Project Description	Division /Campus	Summary of Observations and Recommendations	Status & Summary of CAPs
22-001A	In Progress	External Penetration Test Follow-up	OIT	Review actions taken on recommendations made in an external IT penetration test performed in FY 2021.	
22-016A	7/20/22	IA assisted the TSTC Foundation with procuring an audit of the newly constructed Griffith Hall. This was not a College audit.	TSTC Foundation	The audit identified $278,281 in disallowed amounts billed and paid eligible for recovery.	Contractor agreed to the overpayments. Payments will be recovered on the final billing.
22-019I	6/3/22	Payment Fraud Investigation	Procurement Services	Investigated an $87,400 payment made to a person who submitted fraudulent payment instructions. $79,662.52 was recovered. This was a phishing scam.	Supplier identity verification has been outsourced, and quarterly training of procurement staff to recognize fraudulent requests.

22-027I	3/24/22	Dental Hygiene Investigation	Dental Hygiene Program	Reviewed controls governing fees charged to students. Determined controls needed to be improved to segregate responsibilities over the collection and disbursement of these fees.	All payments will be made to the Cashier's Office, with funds being recorded in a Departmental account.
22-037A	9/9/22	Audit of Foundation Controls	Accounting/ Foundation	Reviewed controls to ensure a married couple's responsibilities do not create a control problem. All controls are appropriate. No concerns were noted.	

IV. External Audit Services Procured in FY 2022

There was one delegated request in FY 2022 for an audit to be performed by a third-party provider. The following schedule summarizes that project.

Auditor	Date of Delegation	Project Description
Workforce Talent Educators Association	5/10/22	Perform an audit designed to help TSTC understand and communicate its strengths and opportunities of its instructional programs in regards to career building. Workforce outcomes, quality management processes, and instructional program competency assessments will be within the scope of the audit. All of this work is to leverage areas of strength and identify opportunities to improve processes to better serve the employers of the State of Texas in line with TSTC's charter outlined in Chapter 135. The audit was ongoing at 8/31/2022.

V. Internal Audit Plan for FY 2023

The plan was developed through a collaborative effort between Internal Audit, Executive Management, Senior Management, and the Board of Regents. Multiple activities and functions throughout the College were assessed for financial, fraud, regulatory/compliance, and sensitive information, and COVID-Related risks. TAC 202 and technology risks were also considered in the planning. Management and the Board were also requested to provide a list of specific audits they wanted performed. All regulatory-required audits were included in the Audit Plan. Other than the areas actually selected for audit, consideration was given to risks associated with purchasing and procurement card use, workforce development, dual enrollment, fleet management, and audits of the various construction contracts.

A limited scope audit related to benefits proportionality is scheduled again for FY 2023, as is another contract audit. The TEC §51.9337 (Contracting) Audit is intended to satisfy the annual contracting audit requirement. Our planning process yielded the following audit plan for FY 2023:

Audit Name	Budgeted Hours
TEC §51.9337 (Contracting) Audit – satisfies annual audit requirement of contracts	350
American Rescue Plan Act – Higher Education Emergency Relief Fund III	350
Audit of Remote Work Processes and Procedures	350
Accounts Payable Audit	300
Audit of the Waco Physical Plant	500
Audit of the Harlingen Physical Plant	500
Payroll and Benefits Proportionality Audit	500
Fixed Asset Verification	1400
Sick Leave Administration	400
Internal Network Penetration Test (Harlingen campus)	160
Internal Network Penetration Test (East Williamson County campus)	160
Internal Network Penetration Test (Waco campus)	160
Audit of General IT Controls - satisfies audit requirements related to technology risks and TAC 202	450
T-Drive Audit - satisfies audit requirements related to technology risks and TAC 202	400
Quarterly Follow-up of TAC 202 Controls	100
Construction Project Audits	Will be outsourced

The FY 2023 Audit Plan was approved by the Board of Regents on August 18, 2022, by Minute Order #IA 01-22(c).

VI.   Reporting Suspected Fraud and Abuse

TSTC has taken the following actions to implement the fraud detection and reporting requirements of Section 7.09, page IX-38 of the 87th Legislature's General Appropriations Act, and Texas Government Code, Section 321.022:

●   The College's website describes how to report suspected fraud, waste and abuse to the State Auditor's Office. A link to the State Auditor's Office fraud hotline is included, as is the hotline telephone number.

●   A confidential *internal* fraud hotline is also available for people to report suspected fraud, waste and abuse. This hotline is administered by Internal Audit.

●   Statewide Operating Standards GA 1.15, GA 1.16, and GA 1.17 have been adopted that detail responsibilities to prevent/detect fraud, how to report suspected fraud, and describe the College's other expectations in regard to fraud, waste, and abuse. Those Standards are available through the College's website.

●   In compliance with the reporting requirements of fraud, waste, and abuse, the College reports all instances of confirmed fraud, waste, and abuse to the SAO.

VIII. External Quality Assurance Review

An External Quality Assurance Review of the Internal Audit Department was completed on May 17, 2021, by Carole M. Fox, CPA. Ms. Fox is the Chief Audit Executive for the Texas State University System. She is entirely independent from all auditors employed by the TSTC Internal Audit Department.

The results of the review indicated that TSTC Internal Audit Department generally conforms to standards. The Department was also commended for its well-crafted audit charter, and the level of accessibility to the Board of Regents and the Chancellor. A copy of the original report is attached.

May 17, 2021

Mr. Jason D. Mallory, Director of Internal Audit
Texas State Technical College
3801 Campus Drive
Waco, Texas 76705

Dear Mr. Mallory,

At your request, I performed an external quality assurance review on the Internal Audit Department of the Texas State Technical College (TSTC). The review included an independent validation of the assertions and conclusions made in the *Internal Quality Assessment Review Report* issued by Ms. Tahlia Pena, Audit Manager, on November 6, 2020.

The primary objective of the review was to provide an opinion on whether the internal auditing program, overseen by you, achieves the basic requirements expected of internal auditing activities at all State of Texas institutions of higher education. Those requirements are set forth in the *Texas Internal Auditing Act* (Texas Government Code, Chapter 2102), the Institute of Internal Auditors' *Code of Ethics* and *International Standards for the Professional Practice of Internal Auditing*, and the U.S. Government Accountability Office's *Generally Accepted Government Auditing Standards.* For purposes of this review, I collectively refer to these as "the *Standards*". In acting as a validator, I am fully independent of TSTC and have the necessary knowledge and skills to undertake this engagement.

Opinion Rating Definitions
The rating system used for expressing an opinion for this review is defined by the *Standards*, and provides for three levels of conformance: generally conforms, partially conforms, and does not conform.
   ➢ ***Generally conforms*** means that the Internal Audit Department has the relevant structures, policies, and procedures in place and an audit charter that complies with the *Standards* in all material respects; however, opportunities for improvement may exist.
   ➢ ***Partially conforms*** means the Internal Audit Department is making good-faith efforts to comply with the *Standards*, but falls short of achieving some major objectives. This will usually represent that significant opportunities for improvement are needed in effectively applying the *Standards*.
   ➢ ***Does not conform*** means the internal audit activity is failing to achieve many or all of the *Standards'* objectives. These deficiencies will usually have a significant impact on the internal audit activity's effectiveness and its potential to add value to the organization.

Scope and Work Performed
The review was performed in accordance with the State Agency Internal Audit Forum *Peer Review Guidelines* using the *Master Peer Review Program*. The scope included all TSTC internal audit activities from September 2017 through August 2020, and consisted of the following:
   ➢ A review of the self-assessment documents,
   ➢ Discussions with you,

- ➢ Interviews with the Board Chairman (also the former Audit Committee Chair), the former Chairman of the Board, the Chancellor, and members of the TSTC Leadership Team,
- ➢ A survey of a sample of managers who recently participated in internal audits;
- ➢ A survey of all internal audit staff, including you, and
- ➢ A review of the audit working papers for four audit projects completed during the review period.

Results and Opinion

Based upon the self-assessment documents, interviews, survey results, and the review of audit working papers, I concur with the assertions and conclusions stated in the *Quality Assurance Review Self-Assessment Report* dated November 6, 2020 that the internal audit activity at TSTC generally conforms to the S*tandards*.

In my opinion, the TSTC Internal Audit Department **generally conforms** to the *Standards* for the period under review and no significant opportunities for improvement were observed. This opinion, representing the best possible evaluation, means that there are in place the relevant structures, policies, and procedures, including the processes by which they are applied, that comply with the *Standards* in all material respects.

Key Observations

As required by the *Standards*, TSTC has a well-crafted audit charter that clearly defines the audit function's purpose, authority, and responsibility. The Director and audit staff have unrestricted access to all TSTC personnel, records, and property. Results of a confidential survey of auditees indicate a high degree of confidence in the audit function, with many respondents commenting on the professionalism of the audit team. The Director has full and free access to the Board Chairman, the Audit Committee Chair, and the Chancellor; in fact, the level of accessibility is commendable and noteworthy, as it contributes to an enhanced governance structure at the TSTC.

I would like to express my thanks for the time and assistance given by you and your staff and other representatives of the TSTC during the review.

Sincerely,

Carole M. Fox

Carole M. Fox, CPA
Chief Audit Executive
Texas State University System

November 10, 2022
Mr. Tony Abad, TSTC Audit Committee Chairman
Texas State Technical College
Waco, Texas 76705

SUBJECT: Information on Internal Audit's Program of Quality Control

Mr. Abad:

The Institute of Internal Auditors' *Professional Practices Framework* requires I provide you information annually on our quality control program for internal auditing. We have established a program that ensures independence, competency, and compliance to auditing standards. That program includes the following:

- Required annual continuing education for each staff member: In FY 2022, all staff obtained at least 40 hours of professionally relevant continuing education.
- Professional certification(s) and Education: Departmental staff hold undergraduate degrees in Accounting, Management, and Cybersecurity. Two staff also hold MBAs. Professionally recognized licenses and certifications held include 1 CPA, 2 Certified Internal Auditors, and a certification in control self-assessment. Additionally, recognitions as Certified Information System Auditors are also being pursued.
- Internal and external quality assessment reviews: An external review was performed in FY 2021 that resulted in "Generally Conforms to Standards" opinions. The external review was performed by Carole Fox, CPA. She is the Chief Audit Executive for the Texas State University System.
- Reliable and sufficient documentation for all audit reports and opinions: I supervised all FY 2022 audits, and conducted working paper reviews before any reports or opinions were issued.
- Policy and procedures manual: All auditors are in possession of the manual, and acknowledged their responsibilities in writing prior to the fiscal year. That manual was reviewed and updated throughout the year as procedural changes were enhanced, with staff being promptly informed. We have a designated staff member that periodically reviews all internal policies governing our work practices.
- Independence statements. In FY 2022, all auditors acknowledged their independence in writing. Formal procedures are established to address any potential conflicts of interest that may arise.
- Membership in professional organizations. The Department is a member of the *Institute of Internal Auditors (IIA),* the *Association of College and University Auditors (ACUA),* and the *Texas Association of College and University Auditors (TACUA).* One staff member still serves on the Board for TACUA.
- Client surveys. In FY 2022, client opinions of our work were sought after each audit. All responses were generally good to exceptional.

Sincerely,

Jason D. Mallory
Director of Audits

November 10, 2022

Mr. Tony Abad, Audit Committee Chairman
Texas State Technical College
Waco, Texas 76705

SUBJECT: Annual Confirmation of Organizational & Individual Independence

Mr. Abad:

The Institute of Internal Auditors' *Professional Practices Framework* requires that I confirm annually to you that the Internal Audit Department and its staff are organizationally independent within TSTC to assure you that audit reports and other opinions I offer you are free of interference from management.

I attest that the Internal Audit Department has a reporting structure which promotes organizational independence. The current structure requiring me to report functionally to the Chairman of the Audit Committee, but administratively to the Chancellor, achieves the requirements of the *Professional Practices Framework.* I do not feel any barriers exist which prevent my direct communication and interaction with you. Also, there has not been any instance in which management has attempted to limit the scope of the internal audit role, interfere with work necessary to offer opinions, or unduly influence communications that you receive.

And while not specifically required to be confirmed, I also attest, to the best of my knowledge and belief, that my staff and I are free from any personal impairments which might present a conflict of interest. Everyone is expected to maintain independence of mental attitude in the conduct of all assigned work, to be objective, fair, and impartial, and to conduct themselves appropriately at all times. To limit and identify personal impairments, Internal Audit Department employees cannot have any operational responsibilities outside of the Internal Audit Department. They must also annually acknowledge their responsibilities in writing, and report any situation they feel might jeopardize their objectivity.

Sincerely,

Jason D. Mallory
Director of Audits

Internal Audit Department

Audit Report

Audit of Foundation Controls (Limited Scope) (22-037A)
TEXAS STATE TECHNICAL COLLEGE

September 9, 2022

This audit was conducted in accordance with the
International Standards for the Professional Practice of Internal Auditing
Of the Institute of Internal Auditors.

Executive Summary

Internal Audit has completed a limited scope audit of select controls relied upon by the Foundation. We tested controls that reasonably prevent and detect inappropriate activity that could occur as a result of collusion between a married couple who hold key positions within the Foundation and the College's accounting department. Each year the Chancellor includes this as a risk to be audited periodically when he provides input to our Annual Audit Plan. While there has not been a specific concern expressed about any transaction, this audit provides independent assurance of the controls that are relied upon to manage inherent risks associated with this close relationship. A periodic audit also demonstrates the organizations' awareness of the risks, and their desires to ensure they are well controlled. Furthermore, management has requested similar audits in the future as we determine appropriate.

We tested access to the accounting system used by the Foundation, access to Foundation bank accounts, and oversight of key accounting functions. We also reviewed several transactions in fiscal year 2022 to identify any potential transactions where either of these individuals may have benefited personally.

We determined there are adequate controls in place to reasonably ensure all transactions related to the Foundation are not compromised by the relationship. We determined that the College's accounting executive did not have any capability to affect transactions associated with the Foundation. He does not have access to the Foundation's accounting system or bank accounts, and does not approve any accounting activity. Both individuals are mindful of the risks, and have been deliberate in maintaining a separation between their work responsibilities.

Introduction

The TSTC Foundation supports TSTC's 10 campuses across the state, its students, career programs, faculty and staff. It supports the critical needs of students (scholarships, hardships, tools and equipment) and provides funds to enhance the College's ability to provide new and emerging technical programs to support the Texas workforce. This support is used to help improve student success, strengthen the technology of labs, as well as to provide flexibility to the priorities of the College to support the state's growing workforce demands.

Elizabeth Wooten is the AVC/External Relations, as well as the CEO for the Foundation. Her spouse, Chad Wooten, is the AVC/Finance for the College.

Objectives

The overall objective of the audit was to ensure adequate controls exist to reasonably prevent inappropriate activity that may occur because of the family relationship between the Foundation CEO and the AVC/Finance.

Scope & Methodology

The scope of our audit included all financial and accounting related controls that were in place at the time of this audit. All transactions in fiscal year 2022 were within the scope of our testing. Our testing consisted of reviewing software access, bank signature cards, accounting responsibilities, Foundation Board minutes, and bank reconciliations.

General Observations

Management has been deliberate to ensure no Foundation related functions are performed by the AVC/Finance or his direct reports, and to eliminate any capabilities to access Foundation transactions. The VC/CFO for the College oversees all accounting transactions that are recorded by the Foundations accountant, who reports to the Foundation CEO. The financial statements for the Foundation are audited annually by an independent accounting firm, with unqualified opinions being rendered for several years. The auditor in the most recent audit recommended more oversight be provided over the Foundation accountant to ensure she does not perform conflicting duties. Management implemented those recommendations, demonstrating their commitment to strong controls.

Everyone we interacted with in this audit was helpful in explaining processes and providing assistance. The Foundation accountant was especially responsive to all requests that we made.
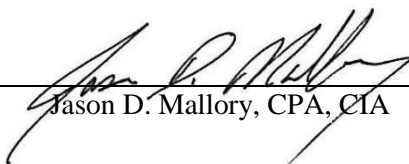
Summary of Finding

No exceptions were identified.

Opinion

Based on the audit work performed, adequate controls exist to reasonably prevent and detect inappropriate activity that may occur because of the family relationship between the Foundation CEO and the AVC/Finance. Furthermore, we did not identify any transaction that were not for the direct benefit of the Foundation and/or College.

We would like to extend our appreciation for the time and assistance given by management and employees during this audit.

Submitted by:

Jason D. Mallory, CPA, CIA	September 9, 2022
	Date

To: Audit Committee
From: Jason D. Mallory, Audit Director
Subject: Follow-up Results for the External Network Penetration Test and Web
                Application Vulnerability Scan, and the Web Application Penetration Test
Date: September 21, 2022

Between September 7, 2020, and September 30, 2020, AT&T Cybersecurity Consulting performed external penetration tests of the College's internet-facing network infrastructure and select applications. The test was designed to simulate attacks from an external adversary, and to identify network and application vulnerabilities that could be exploited.

There were 2 reports issued that described each project, their scopes, and any findings that warranted attention from the IT staff. These reports are not attached because of the sensitive nature of information they include, but are available upon request.

The purpose of this memorandum is to communicate the results of follow-up testing Internal Audit performed to verify any deficiencies were resolved.

External Network Penetration Test and Web Application Vulnerability Scan
Issued on September 30, 2020, this test identified 2 high risks and 2 moderate risks that required attention.

The first high risk that was identified related to the presence of a SQL injection vulnerability that allowed the consultant to obtain unauthorized access to Database Management System (DBMS) stored information. The other identified high risk involved an unsupported instance of Hypertext Preprocessor (PHP) running on a host. This could introduce additional vulnerabilities.

The moderate risks included account enumeration and weak Transport Layer Security (TLS) configurations.

Internal Audit determined that appropriate corrective actions were taken for each of the 4 risks.

Web Application Penetration Test
Issued on September 25, 2020, this test identified 1 high risk, 3 moderate risks, and 1 low risk for one system they tested.

The most serious risk related to the lack of a lock out threshold for the system. The absence of an account lockout feature can give an attacker an infinite number of attempts to login to the system

using any account that is known (i.e., 'brute force' attack). There are many scripts and tools that automate this type of attack available on the Internet that can be used against a web-based application.

The moderate risks related to weak password criteria, account enumeration, and external service interaction.

The low risk indicated that the system auto-completed login forms.
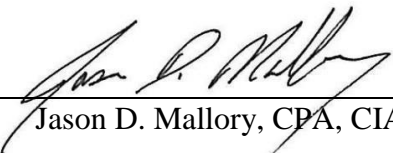
Internal Audit determined appropriate corrective action was taken on the high risk and the 2 moderate risks related to account enumeration and external service interaction. The moderate risk related to password criteria was found to be substantially complete.

For the low risk that was identified, a request was submitted to the system's vendor to consider enhancements in future software updates to address the risk. The vendor was receptive but non-committal. Nevertheless, we determined that current controls for this risk are appropriate given the nature of the risk. Additionally, the College is using the most current version of the software. The security of that software has been certified through an external audit.

Overall, we found appropriate action was taken on all risks that were identified in the external tests.

We commend the IT staff for engaging these tests periodically to proactively harden the College's network and systems against the limitless and constantly evolving cyber-attacks. These tests, along with internal ones performed by Internal Audit and the other technology controls that are in place, demonstrate a commitment to protecting College resources and data.

Submitted by:

_____   September 21, 2022
Jason D. Mallory, CPA, CIA   Date

cc: Mike Reeser, Chancellor/CEO
         Ricardo Herrera, VC/CSSO
         Shelli Scherwitz, Executive Vice President/OIT
         Larry McKee, Executive Director/OIT Compliance

Internal Audit Department

Audit Report

Bookstore Audit (22-034A)
TEXAS STATE TECHNICAL COLLEGE
Marshall Campus

September 26, 2022

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

Executive Summary

We recently completed an audit of the Bookstore (Bookstore) on the Marshall campus. The audit verified various accounting controls related to revenue, costs of goods sold, inventory, cash, accounts receivable, sales tax payable, and accounts payable. We tested access to the Bookstore facilities and merchandise, IT access, and the general effectiveness and efficiency of its operations. Finally, we validated select general policy requirements (fixed asset custody, employee training, and leave usage). The majority of our audit focused on transactions and the state of operations in fiscal year 2022 through May 31, 2022. However, we included select information from prior fiscal years to understand the operations in an historical context.

We determined the following:

Accounting controls	Controls were generally well designed, but, some warranted attention. In a management letter, we offered a recommendation related to the recordation of credits owed by vendors due to a minor error we found.
Security of merchandise and cash	Controls were sufficient to reasonably protect both merchandise (books, tools, clothes, etc.) and cash from theft. Our surprise counts of both inventory and cash were successful. Additionally, we were able to fully reconcile book buy back cash on hand.
Access to the facility	Facilities were secured with locks and security cameras. The access to these was limited to appropriate personnel.
Access to Colleague, Workday, and the Point of Sale System	Access to these systems by Bookstore personnel was appropriate.
Taxable items for sale	In a management letter, we recommended certain items coded as non-taxable in the point of sale system be reviewed. Some items, like cleaning supplies, looked like taxable items to us. We do not feel that recommendation was necessary to address in this report because the volume of these sales is insignificant.
Employee leave	All leave was handled in accordance to policy.

Required training	All required trainings were completed by employees by the end of the fiscal year.
Prompt payment of invoices	Found some payments that were paid outside of the 30-day requirement due to invoices not being processed timely. However, the implementation of Workday has made this process more efficient and effective.
Effectiveness and Efficiency	Found the operations effectively provide students the books and other supplies they require. We calculated inventory turnover rate and revenue per employee for fiscal years 2019 through 2022 to gauge efficiency. We found inventory turnover and revenue per employee decreased significantly in FY 2020, and continued to decline. The COVID shutdown in FY 2020 and changing College operations have contributed to the decline.

Introduction

The Bookstore stocks all supplies students need to be successful in their program of study, to include text books, tools, school supplies, College branded clothing, gifts, and snacks. In addition to the physical inventory on hand, the Bookstore also facilitates the Inclusive Access program which allows students to purchase digital learning materials instead of physical textbooks. The Bookstore is open Monday through Friday, and offers extended hours during peak times, such as registration and beginning of each semester. Purchases are paid by cash, credit cards, through financial aid, and by various sponsorships.

The following table illustrates revenue by merchandise type over 3 fiscal years:

Revenue by Merchandise Type

Type	FY 2020	FY 2021	FY 2022*
Books	$98,381.46	$81,602.94	$42,221.44
Tools	$16,267.81	$18,914.79	$19,323.42
Food	$36,740.64	$8,254.78	$21,213.70
Clothes, electronics, graduation supplies and misc.	$25,606.07	$20,041.07	$20,029.02
All	$176,995.98	$128,813.58	$102,787.58

* This revenue excludes June, July and August 2022. The highest sales volume is typically generated in August.

The following table illustrates the Cost of Goods Sold over the same 3 years, along with the associated inventory turnover ratio:

COGS & Inventory Turnover Ratio by Fiscal Year

	FY 2020		FY 2021		FY 2022	
	Amt	Ratio	Amt	Ratio	Amt	Ratio
All	$130K	0.95	$95K	0.58	$81K	0.49

The Bookstore has a staff of two that includes the Manager, and a part time customer service associate. In fiscal years 2019, 2020, 2021, and 2022, the employee costs were $74,009, $74,116, $74,477 and $56,334, respectively. The revenue generated by employee for each fiscal year was $166,972, $120,7923, $100,415, and $97,058 respectively. Stated differently, the Bookstore generated $3.38 for each dollar of employment costs paid in FY 2019, $2.44 for each dollar of employment costs paid in FY 2020, $2.02 for each dollar of employment costs paid in FY 2021, and $2.58 for each dollar of employment cost paid in FY 2022. For FY 2022, amounts included are only through May 31, 2022.

The Bookstore generated a net operating income (loss) in fiscal years 2020, 2021, and 2022 (as of May 31, 2022) of ($39,922), ($42,253.12), and $11,146 respectively. Again, at the time of this audit, the final operating results were not available for FY 2022.

Objectives

The objectives of the audit were to ensure accounting controls were appropriate over Bookstore related accounts, the Bookstore operated effectively and efficiently to achieve its purpose, and to verify select compliance objectives related to IT access, leave usage, fixed asset custody and training are being met.

Scope & Methodology

The scope of our audit included all Bookstore transactions and processes in FY 2022 through May 31, 2022. To accomplish our objectives, we documented key internal controls, observed various practices and procedures, performed surprise cash and inventory counts, reviewed relevant general ledger and Point of Sale system reports, and spoke with Bookstore and Accounting staff with bookstore related responsibilities. We also reviewed reports relating to IT access and facility safeguards. We utilized various Statewide Operating Standards in our compliance testing to include SOS FA 1.6 Taking of Consumable Inventories, SOS FA 2.1 Establishment and Control of Petty Cash, SOS FA 2.02 Control of Cash, Cash Receipts, and Cash Refunds, SOS FA 1.19 Real and Personal

Property Accountability, SOS HR 2.3.12 Employee Leaves and Holidays, and SOS HR 2.3.13 Family & Medical Leave.

General Observations

The Bookstore staff provides excellent customer service by getting to know students who come in daily. The Marshall campus does not have a cafeteria, so the Bookstore provides drinks, grab-and-go snacks, and some prepared food items. The facilities are appropriately restricted to authorized personnel, and book inventory is stored in a restricted area to limit pilferage. The manager has a strong process for ensuring the appropriate inventory is on hand to support student's needs.

The point of sale system accurately records sales and sales tax at the proper amounts. Accounting personnel have processes in place to reflect operating results. The implementation of Workday has presented some challenges to the Accounting staff that they are actively addressing. Staff from the Bookstore and Accounting were responsive to our requests and professional in all interactions. It is obvious they take pride in the services they provide.
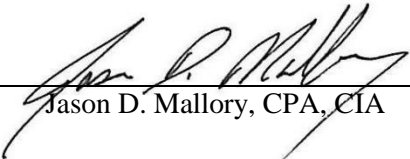
Summary of Finding

No material exceptions were identified.

Opinion

Based on the audit work performed, accounting controls are appropriate to ensure Bookstore operating results are accurately reflected in accounting records. The Bookstore operates effectively and efficiently, and they protect inventory and cash they have in the store. Finally, no significant compliance issues were noted as they related to IT access, leave usage, training, and asset custody.

We would like to extend our appreciation for the time and assistance given by management and employees during this audit.

Submitted by:

_____   _____
Jason D. Mallory, CPA, CIA   September 26, 2022
                                                                            Date

Internal Audit Department

Audit Report

Internal Network Penetration Test (23-004A)
TEXAS STATE TECHNICAL COLLEGE
Harlingen Campus

September 30, 2022

This audit was conducted in accordance with the
International Standards for the Professional Practice of Internal Auditing
Of the Institute of Internal Auditors.

Executive Summary

Between August 15, and September 2, 2022, we performed vulnerability scans and penetration testing of the College's internal network on the Harlingen Campus.

The primary objective of this project was to ensure sensitive information stored and processed by primary systems, and systems directly supporting the confidentiality, integrity, and accessibility of those systems, have controls in place to detect and prevent attacks from unauthorized individuals on the campuses. Physical and logical security controls, to include the actions and habits of personnel, were targeted in this project. We conducted a similar test on the Harlingen campus in fiscal year 2020. We relied solely upon public information we collected through the internet to perform that test. In this one, we selectively sampled employees with probable access to sensitive data using our knowledge of internal information. We selected this approach to get a broader understanding of actions employees would take when confronted with potential cyber risks.

We tested end user training effectiveness by calling and sending emails (known as social engineering and phishing) to select individuals. We requested sensitive information that would never legitimately be sought. Target information in these social engineering tests were Workday logon credentials and procurement card data. We also attempted to have an employee's payroll direct deposit information changed to an unverified account.

We attempted to gain access to privileged systems and information by scanning the network to identify technology flaws such as outdated software versions, tested wireless access points, and searched for available ports connected to the internal network that we could plug in to. We attempted to access computers available to the public to determine whether we could potentially pivot to an area on the network where sensitive information is stored. Finally, we verified personnel completed Information Security Awareness Training the last 3 fiscal years. Both manual and automated testing methods were used to detect and/or exploit potential vulnerabilities. Industry standards noted in the Scope & Methodology section of this report served as our basis.

Our results indicated an improvement over access to restricted areas and sensitive information since our last test. Employees on campus were aware of students/staff coming in and out of buildings that were open to the public, and classrooms available to students. Computers in public areas were restricted requiring either a student or employee user id and password in order to access them, we did not locate any open ports on campus, and staff who were present on campus locked their offices when they stepped away from their desk. The College's open wireless connection limits the range of use not allowing a connection more than 30 yards away from the building, and all other wireless connections required a user name and password in order to authenticate access to the network. We did not find any buildings left unlocked after hours. Information Security Awareness Training required annually is being completed by most of the employees we selected during our testing.

While most people ignored or rejected our social engineering attempts, we were able to obtain 9 employees' logon credentials to Workday, as well as College issued Procurement/Travel card information from 3 employees. All compromised passwords were immediately changed, and all compromised credit cards were terminated. We were able to access the internal network by pivoting from a guest wireless connection outside one campus building, and determined one network printer was using the default username and password. The latter 2 issues were corrected immediately.

Introduction

The Office of Information Technology (OIT) Division, overseen by an Executive Director, assists the College with its operational needs by maintaining secure IT networks, providing end-user support and training, assisting with IT purchases, and maintaining critical databases and offering critical application support.

Internal Audit worked closely with members of the IT Support Operations Department and the Department of Infrastructure Operations. Other than managers, employees in IT were only notified when accounts were compromised or immediate remediation was required. Also, to ensure the integrity of the results, limited people on the campus were notified of our tests prior to us performing them.

With work and instruction mostly operating in a hybrid mode, there were fewer employees/students on the campus. Fewer people decreased the likelihood of risks related to behavioral lapses that could occur. Many of the rooms and areas on the Harlingen Campus were restricted or closed.

Objectives

The objectives of the internal network penetration test were to:
- Ensure primary systems, and systems directly supporting the confidentiality, integrity, and accessibility of primary systems have the controls in place to detect and prevent attacks.
- Ensure unauthorized individuals on campus are unable to access privileged systems or sensitive data.
- Verify the effectiveness of end-user training on threats related to information security.
- Allow the College to gain insight into real-world attack vectors that may have not been previously considered or tested.

This test was not intended to verify all risks the campus may face during an attack. Instead we focused on select employees, and designed tests that mirrored known real-world attack methods.

Scope & Methodology

The scope of the penetration test included the physical and logical securities of core network equipment, access network equipment, and networking closets located on the Harlingen Campus. It also included employee behavior, especially their awareness of and vigilance against potential

related attacks that compromise IT systems and other sensitive data. The following industry standards served as our methodology:

- IS Benchmarks - Baseline Configurations for Secure Operating System and Application Deployment
- NIST Configuration Baselines - Baseline Configurations for Secure Operating System and Application Deployment
- NIST 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations
- NIST 800-115 - Technical Guide to Information Security Testing and Assessment

To accomplish our objectives, we sent emails and made telephone calls requesting Workday logon credentials to 45 employees who have access to sensitive information. We also sent emails to 15 other employees requesting they provide their Procurement/Travel credit card information to us. Finally, we attempted to have payroll direct deposit information changed by requesting a change through the Payroll Department via email. For our other tests, we scanned network services, attempted to access areas that should be restricted, tested open ports and reviewed available training documentation.

General Observations

Most employees rejected or ignored our social engineering attempts. Users must logon to public computers. Rooms housing network equipment were locked, and required a badge or pin code to access them. Offices in various buildings were locked when employees stepped away. Wireless networks had a very limited range outside of buildings, which reduced the possibility of people performing scans and attacks without being detected. We did not locate any open ports that allowed us to perform network scans. Staff was alert to our presence on campus. We were approached in several buildings and asked if we needed assistance or why we were in the building. We were not allowed to use any of the private rooms or computers in the Learning Resource Center without presenting a student ID. We did not identify any areas after hours that we could access, and the Police had a noticeable presence on campus.

We noted several actions that are commendable. An employee in the Payroll Department refused to initiate a direct deposit change. She insisted the employee who made the request submit it through Workday. She ultimately contacted the employee on his cell using a number on record to verify the legitimacy of the request. This cell number was not present in the phishing email, indicating she was aware of the need to use information on file rather than in the bogus request.

Procurement Services immediately cancelled procurement and travel cards that were reported as compromised. Every employee who provided this information, interestingly, immediately reported the matter. Procurement Services also appropriately attempted to have a College-wide notification sent to inform the campus community of the ongoing attack. [Note: IT did not send an email because select members were aware of our test, and did not want to disrupt it.]

OIT contacted all employees who provided logon credentials to initiate password changes. Personnel were helpful in planning this test, and helped maintain its confidentiality while it was underway. We also noted that OIT has implemented features in the email system that help identify spam emails and emails that are potentially fraudulent. The emails that were acted upon were flagged as suspicious by the system. And, OIT has actively assisted with more detailed training to identify specific scams, such as the ones we tested.

Summary of Finding

There needs to be a heightened awareness of cybersecurity risks College-wide. We were able to compromise 20% of the employees we tested through our enhanced social engineering tests.

Opinion

Based on the audit work performed, assets and sensitive information are generally well protected on the Harlingen Campus. However, there is a critical need to raise awareness on this campus of social engineering attacks and scams. The College, as a whole, would probably benefit from such an awareness campaign, as actual attacks have increased.

We would like to extend our appreciation for the time and assistance given by management and employees during this audit.

Submitted by:

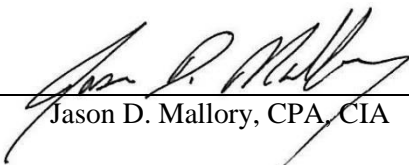|	
Jason D. Mallory, CPA, CIA	September 30, 2022
	Date

Finding #1: There needs to be a heightened awareness of cybersecurity risks College-wide. We were able to compromise 20% of the employees we tested through our enhanced social engineering tests.

Criterion: We made telephone calls and sent emails to 61 employees, primarily on the Harlingen Campus. We tested each of the employees in this sample in one of 4 ways.

Our first test involved sending 30 employees an email attempting to trick them in providing their Workday logon credentials.

Our second test target 15 employees via a telephone call also attempting to persuade them to provide their Workday logon credentials.

In our third test, we sent emails to 15 people who likely had procurement cards, requesting they provide the number, security code, and expiration date of their card(s). We had no insight into whether the employees actually held cards.

Finally, we tested the Payroll Department by requesting the direct deposit information for an employee be changed. We performed this test to ensure all required verification steps were taken prior to making any changes.

We intentionally created an urgency to respond, and tested at times we knew people would be busy with other responsibilities. From our experience with real frauds, these 2 characteristics are always present.

Our specific methods are not included in this report so as to limit copycat attempts.

Our tests yielded the following results that need to be addressed:

- Seven employees provided their logon credentials to the Workday application by submitting information in response to the phishing email we sent in our first test.
- Two employees provided us their Workday logon credentials over the telephone via our social engineering telephone calls in the second test. One employee failed this same test in fiscal year 2020.
- Three employees provided their Procurement/Travel credit card information via telephone in response to the email we sent in our third test.

The fourth test related to the direct deposit change request was unsuccessful. The employee refused to make any changes without first contacting us using information she had on file.

The following were also noted, but immediately corrected by OIT:

- We were able to access the internal network from the TSTC Guest wireless access point outside of one of the buildings.
- We were able to access a network printer using a default administrator username and password.

We communicated our tests with all 61 employees who were tested, and sent follow-up communications to those 12 who provided information. Each supervisor of those who failed committed to counseling their employees and to educating their other employees about our tests and the risks they were aimed. We included examples of our actual methods, and pointed out the clues we intentionally put in our communications that should have alerted them that the emails and telephone calls were scams. We provided this level of transparency in an effort to raise their awareness and vigilance.

Twelve of 61 (20%) employees we tested provided information that could have caused significant data or financial loss to the College had these been real attacks. Every employee we tested recently completed the required annual cybersecurity training. OIT is providing specific trainings to enlighten employees on the types of scams we tested. And, College email blocks spam and identifies emails that are potentially fraudulent. Despite these controls and processes, this audit suggests more awareness is still needed.

Consequences: Increased risk of inappropriate access to sensitive data.

Possible Solutions: We recommend the specific employees who provided their logon credentials be counseled, and the College implement a marketing style awareness campaign to compliment and reinforce the required annual training every employee receives, the specific communications OIT periodically sends regarding phishing attacks, and the other technology related controls that have been implemented.

Management Response

Management of OIT agrees with the observations and recommendations made in this audit. While there are several technology related controls and other processes such as training, employees responding to fraudulent requests remains a main cyber risk. Every internal penetration test Internal Audit has conducted since 2017 has resulted in a few people being compromised. But, their enhanced efforts in this test seems to have exposed that issue to be larger than expected. To help elevate awareness, the OIT Security Department engaged the Communication & Creative Services Department (C&CS) on September 23, to create a College-wide awareness campaign that includes memorable slogans and examples of real fraud attempts. It will incorporate various delivery methods. C&CS agreed that such an awareness approach that is different from the various emails and training provided by OIT might help reinforce known risks and expectations. Larry McKee, Executive Director, OIT Compliance will be responsible for ensuring this awareness campaign is implemented, and that it incorporates sufficient

information to improve employee awareness of the cyber risks and losses the College is exposed to.

To: Audit Committee
From: Jason D. Mallory, Audit Director
Subject: Quarterly Results of Personal Property Verification Audit (23-003A)
Date: October 5, 2022

Internal Audit is in the process of auditing personal property owned by the College. Personal property refers to:

- Capitalized assets that cost $5,000 or more, have a useful life greater than one year, and are depreciated. Examples include furniture and equipment, airplanes, vehicles, and machinery of various forms.
- Controlled assets that cost between $500 and $4,999.99, and are not capitalized or depreciated. They are tracked because they are inherently at more risk of theft, damage, and obsolescence. Examples include sound systems, televisions, computers, and drones. Regardless of cost, hand guns and rifles are always considered controlled assets.

Excluded from this audit are real estate, intangible assets, library books, and historical artifacts.

Texas Government Code, Subchapter L, section 403.2715 (Code) requires the College to account for all assets, including personal property, using the definitions, accounting classification codes, capitalization thresholds, useful lives, and depreciation methods defined by the State Comptroller's Office in their "SPA Process User's Guide". The Code also requires the College to:

- Maintain asset records that accurately reflect all property possessed by the College.
- Designate a property manager to be responsible for the custody of all personal property, and the maintenance of associated records. The CFO is the designated property manager.

The State Auditor has the authority to periodically examine records and property related controls.

The "SPA Process User's Guide" also provides specific guidance on select internal controls, such as the annual inventory of personal property. This guidance, though, seems more aimed at users of the Comptroller's asset accounting system. The Code exempts the College from using that system, so certain parts of the guide are likely not applicable. Current internal controls that are relied upon to achieve accurate records and the safe custody of personal property are currently being refined in College policy.

The primary purpose of this audit is to verify that the recent annual inventory of personal property reflects the actual existence, condition, location, and steward of each recorded asset. Controls that impact this objective, such as training and monitoring of the annual inventory completion status are also being tested. The College's Property Accountability staff has real time access to our daily

test results for easy follow-up with stewards as we identify discrepancies. The following are the results of our tests as of October 5, 2022:

Campus	Total	Sample	Tested	Left to Test	% Left to Test
Abilene	1,172	463	7	456	98%
Austin	19	18	18	0	0%
Breckenridge	183	74	2	72	97%
Brownwood	385	108	17	91	84%
Ft. Bend	1,864	597	0	597	100%
Harlingen	6,675	2,227	219	2,008	90%
EWCHEC	445	118	41	77	65%
Marshall	1,478	483	0	483	100%
North Texas	923	327	1	326	99%
Sweetwater	2,045	676	3	673	99%
Waco	9,259	3,010	482	2,528	84%
ALL	24,448 [Note 1]	8,101	790	7,311	90%

Note 1: This was the total number of assets on 8/7/22 when our sample was selected. This number fluctuates daily due to purchases and disposals, but has consistently remained between 24 and 25 thousand.

Audit Results - Through 10/5/22

.
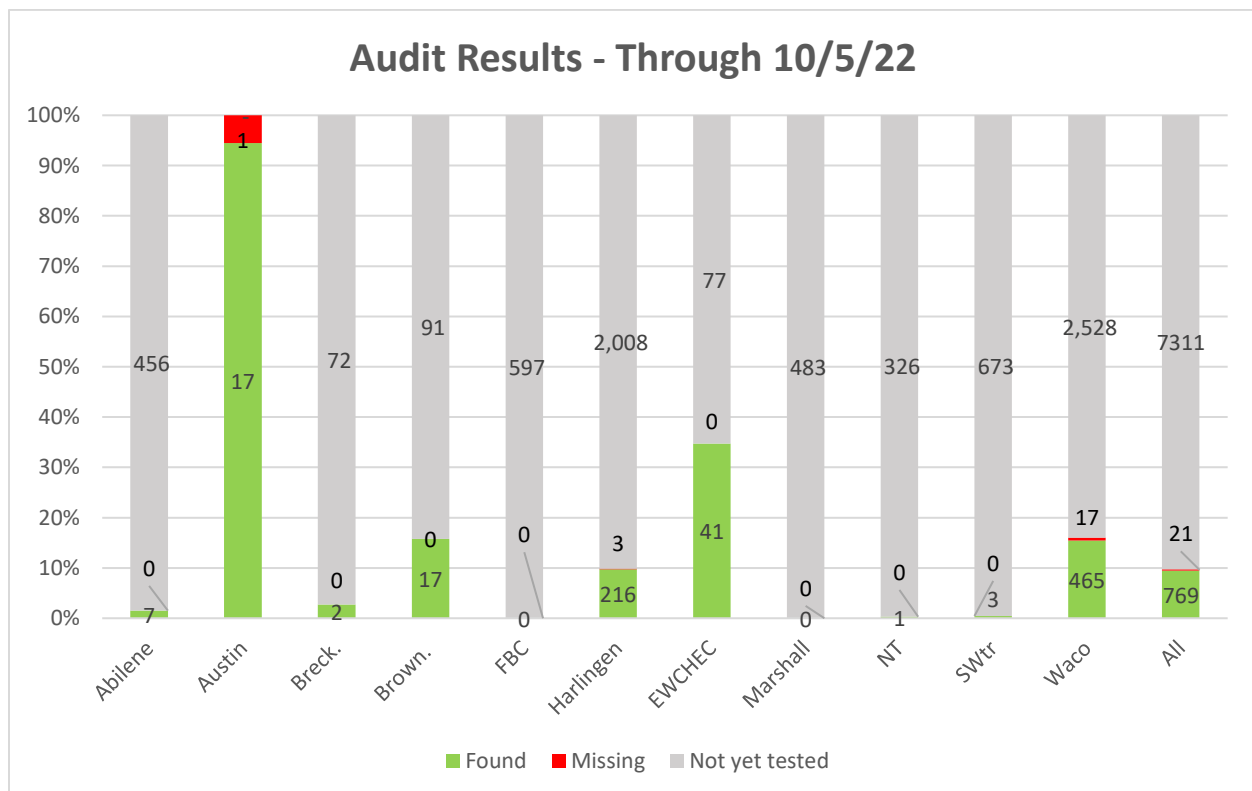
Recording & Tag Exceptions

	Missing	Condition	Location	Not Tagged
ABILENE	0	0	0	0
AUSTIN	0	0	1	2
BRECK.	0	0	0	0
BROWN.	0	0	0	7
FBC	0	0	0	0
HARLINGEN	1	7	8	3
NEWCHEC	0	0	0	0
MARSHALL	0	0	0	0
NT	0	0	0	0
SWTR	0	0	0	0
WACO	8	122	38	9
ALL	9	129	47	21
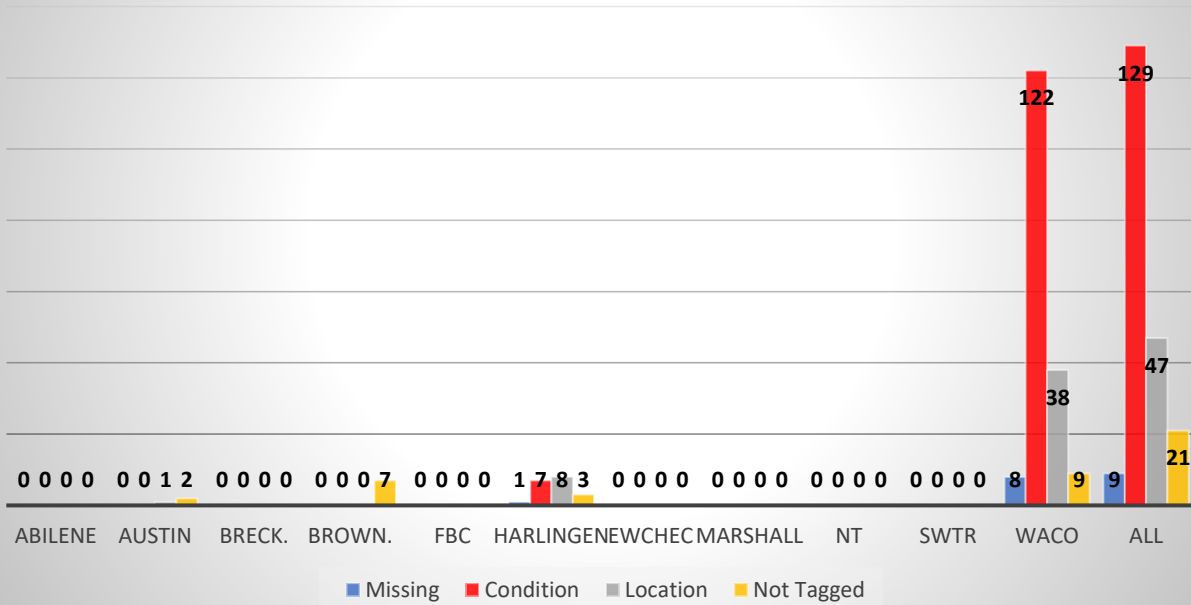
Possible Opportunities for Disposal

	Poor Condition	Not Used
ABILENE	0	0
AUSTIN	1	3
BRECK.	0	0
BROWN.	7	13
FBC	0	
HARLINGEN	17	34
NEWCHEC		35
MARSHALL	0	
NT	0	
SWTR	1	1
WACO	65	65
ALL	96	151
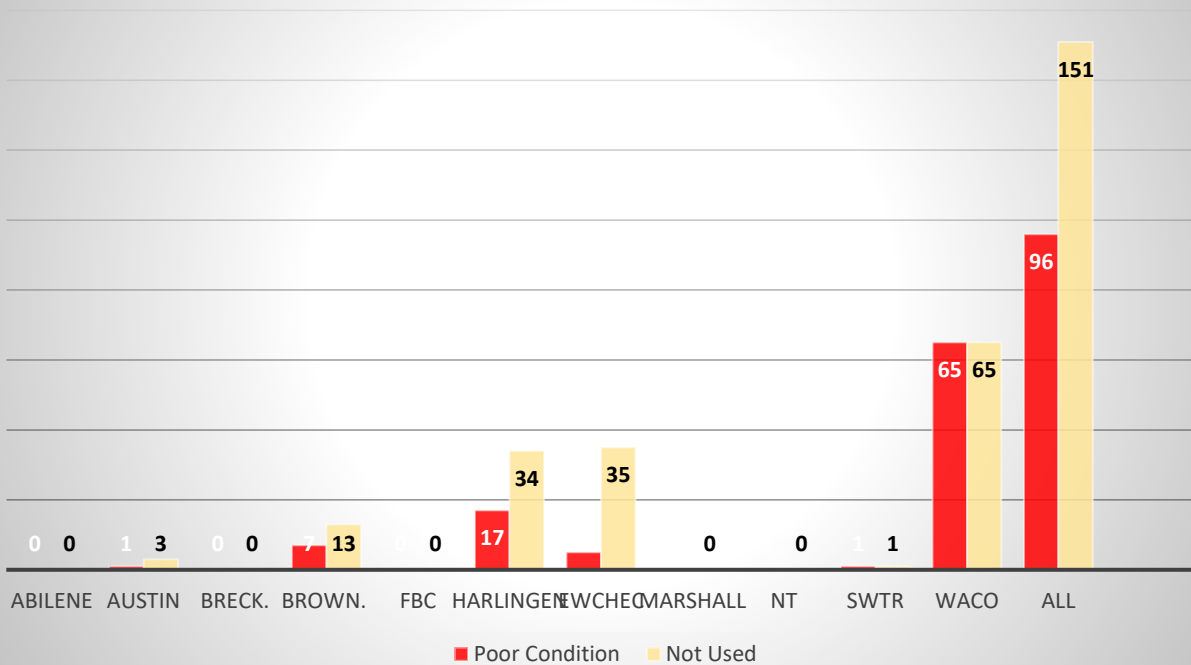
Of the 1,415 asset stewards on record as of the date of this report, 1,215, or 86% have taken their annual inventory of personal property. Our results are not precise because asset records constantly change due to asset and steward additions and deletions. We are confident, though, the completion rate is between 85% to 92%. Workday provides insight into this rate that was not as readily available in years past.

Of the 517 stewards represented in our sample, only 15 did not complete their required training. That represents a successful completion rate of 97%.

The data we are verifying is available in real-time to the Property Accountability staff. The data provides additional insights beyond what are included in this summary report. The staff are using our results to facilitate records improvement with individual stewards. We will review a sample of the deficiencies we noted towards the end of this audit to verify their actual efforts and results.

While it is too early in the audit to offer an overall conclusion, most of the personal property we have tested has been presented for inspection. Nevertheless, we are finding the need for some stewards to update the location and condition of their personal property in Workday. We have also identified personal property that is clearly in poor condition and/or not being used. This property should be considered for disposal to free up resources for other uses, and to reduce holding costs.

cc: Mike Reeser, Chancellor/CEO
        Jonathan Hoekstra, VC/CFO
        Melinda Boykin, EVP/Procurement
        Peggy Wilke, Executive Director/Procurement
        Jan Dudik, AVP/Property Management

An Executive Summary of TAC-202 at Texas State Technical College

The *Texas Administrative Code, Section* 202 (commonly known as TAC-202) creates the minimum standards for IT security at state agencies. TSTC is subject to these requirements.

The *Texas Department of Information Resources*, the chief IT agency in Texas, provides agencies with a resource for fulfilling TAC-202. These guidelines are published in a *controls catalog* that classifies controls as either required or recommended.

There are 135 required controls that agencies must apply to the general IT environment and/or their individual systems. Such required controls relate to access, change management, audit logging, back-up & recovery, maintenance, and various physical safeguards.

TAC-202 is so broad and so comprehensive that agencies across the state struggle to comply with the daunting scope of the rules. Indeed, reaching full compliance can take many years for some while other agencies may never reach the goal.

Since the work cannot possibly be completed all at once, the TSTC approach to TAC-202 has been to first target the high-risk and/or mission critical systems. Then, in turn, the various requirements are addressed in a logical sequence of declining risk levels. This work is ongoing today.

While an internal audit is required biennially, TSTC has elected to practice a higher degree of audit frequency in TAC-202. In a collaboration between Internal Audit Department and the TSTC IT staff, the college has a *continuous* audit process. This approach exceeds the minimum requirements and ensures a better pace of continuous improvement toward final completion.

As a result of these continuous efforts, a detailed database of controls shared by both IT and Internal Audit has been built that memorializes the required controls that have been audited, as well as the current status of their implementation. This database is invaluable in managing and documenting the extensive efforts to comply and ensure IT security.

An executive summary of the progress made by TSTC in TAC-202 is presented quarterly by Internal Audit to the Board of Regents in a report called: ***TAC 202 Compliance – Quarterly Update.*** This report follows.

❖❖❖

![Texas State Technical College logo]

To: Audit Committee
From: Jason D. Mallory, Audit Director
Subject: TAC 202 Compliance – Quarterly Update
Date: October 5, 2022

The purpose of this memo is to provide you the current implementation statuses of IT controls required by TAC 202 tested in numerous internal audits of systems conducted since 2017. Annually, the list of audits of systems will increase as we continue to audit. Each quarter we test select controls which were previously not implemented. From July 1 through September 30, 2022,

9 more required control were implemented for the TWC (7), VPN (1), and Canvas (1) applications. For the systems that are lightly shaded, all controls have been implemented.

RESULTS

General Controls   Original Audit: June 28, 2017

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted Note 1	Total
As of December 2021	63	19	0	4	86

Note 1: Management has elected to not implement controls SC-20 & SC-21 because implementing is too costly, and does not provide additional risk mitigation. Furthermore, they have researched other agencies and institutions of higher education, and no one else has implemented the controls. IA-7 relates to cryptographic modules. There are no systems or environments that use these. Finally, they have elected to accept risks with not fully implementing CM-11 related to fully restricting software from being installed by end-users. They feel that compensating controls such as malware, and the ability to restrict specific downloads from the internet assist with mitigating associated risks.

Colleague   Original Audit: June 28, 2017

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
As of March 2022	38	11	0	0	49

Perceptive Content   Original Audit: June 28, 2017

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted Note 2	Total
As of March 2022	33	15	0	1	49

Note 2: AU-5 requires the system to send an alert when an audit log fails. This system does not have that capability.

Maxient   Original Audit: February 25, 2019

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
As of December 2021	46	3	0	0	49

Google Suite
Original Audit: December 10, 2018

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted Note 3	Total
As of December 2021	38	9	0	2	49

Note 3: AC-7 requires the system to lock for at least 15 minutes after 10 failed logon attempts. AC-8 requires a banner to be displayed that indicates unauthorized access is prohibited before a user signs on. This system does support either of these requirements. The risk of unauthorized access is mitigated by other compensating controls.

Target X
Original Audit: September 30, 2019

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
As of December 2021	48	1	0	0	49

Informatica Server
Original Audit: September 30, 2019

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
As of December 2021	49	0	0	0	49

PrismCore
Original Audit: September 21, 2020

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted Note 4	Total
As of December 2021	42	6	0	1	49

Note 4: AU-5 requires the system to send an alert when an audit log fails. This system does not have that capability.

Informer
Original Audit: April 6, 2021

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
As of June 2022	38	11	0	0	49

VPN
Original Audit: November 22, 2021

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted Note 5	Total
July 2022 – Sept 2022	50	0	0	2	52
April 2022 – June 2022	49	0	1	2	52
Difference	+1	0	-1	0	

Note 5: AU-5 requires monitoring of audit log failures. Implementing this control would require a 3rd party software add-on, which we do not feel the benefit of doing so outweighs the cost. We have a compensating control where we monitor logs monthly. CP-4 requires periodic back-up testing. The testing of this control would cause a disruption to services provided to employees working remotely. There are compensating controls of stored backup configurations. OIT tests the backups before completing any upgrades or updates to the appliance.

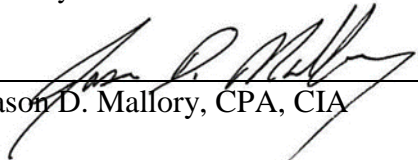**Canvas LMS**   Original Audit: May 20, 2022

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
July 2022 – Sept 2022	38	10	5	0	53
April 2022 – June 2022	37	10	6	0	53
Difference	+1	0	-1	0	

TWC Server   Original Audit: May 16, 2022

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
July 2022 – Sept 2022	46	4	1	0	51
April 2022 – June 2022	39	4	8	0	51
Difference	+7	0	-1	0	

Submitted by:

_____   October 5, 2022
Jason D. Mallory, CPA, CIA   Date

cc: Mike Reeser, Chancellor/CEO
        Ricardo Herrera, VC/CSSO
        Shelli Scherwitz, Executive Vice President/OIT
        Larry McKee, Executive Director/OIT Compliance

August 10, 2022

Jonathan Hoekstra (jonathan.hoekstra@systems.tstc.edu)
Vice Chancellor & CFO
Texas State Technical College System
3802 Campus Drive
Waco, TX 76706

RE: AY 2021 Single Audit Evaluation Management Letter
     CFDA: GEER Upskill & Reskill 84.425C, Perkins Formula-84.048, Perkins Leadership 2-Yr
           84.048

Dear Mr. Hoekstra:

The Texas Higher Education Coordinating Board (THECB), as a federal pass-through entity, must provide due diligence to ensure its subrecipients meet the requirements of the Single Audit Act Amendments of 1996, as prescribed in the U.S Code of Federal Regulations Part 200 (2 CFR Part 200 Subpart F – Audit Requirements), Single Audit Compliance Supplement and Government Auditing Standards.

The purpose of this letter is to issue our management decision regarding findings, if any, related to state or federal funds passed through the Texas Higher Education Coordinating Board that are noted in your organization's Appropriation Year 2021 Uniform Guidance 2 CFR Part 200 Subpart F Single Audit Report and related documentation.

Federal Fund Findings: None
State Fund Findings: None

We greatly appreciate the cooperation and assistance provided by your staff during our review. If you have any questions or comments, please contact Nancy Morales via email at Nancy.Morales@highered.texas.gov or call 512.427.6493.

Thank you for your assistance,

Mark Poehl CPA, CIA, CISA, CFE
Assistant Commissioner, Internal Audit and Compliance
512.427.6161
highered.texas.gov

THECB | Texas Higher Education COORDINATING BOARD

cc: Jason Mallory, Director of Internal Audit (jason.mallory@systems.tstc.edu)

cc: Carliss Hyde, Vice President, Sponsored Programs (carliss.hyde@tstc.edu)
cc: Cindy Reily, Associate Vice President, Office of Sponsored Programs (cmreily@tstc.edu)
cc: Lisa Frenette, Associate Vice President (lisa.frenette@tstc.edu)

August 10, 2022

Jonathan Hoekstra (jonathan.hoekstra@systems.tstc.edu)
Vice Chancellor & CFO
Texas State Technical College - Waco
3801 Campus Drive
Waco, TX 76705

RE: AY 2021 Single Audit Evaluation Management Letter
     CFDA: GEER TEOG Community Colleges 84.425C, GEER TEOG State 84.425C, GEER New
          & Continuing Students 84.425C

Dear Mr. Hoekstra:

The Texas Higher Education Coordinating Board (THECB), as a federal pass-through entity, must provide due diligence to ensure its subrecipients meet the requirements of the Single Audit Act Amendments of 1996, as prescribed in the U.S Code of Federal Regulations Part 200 (2 CFR Part 200 Subpart F – Audit Requirements), Single Audit Compliance Supplement and Government Auditing Standards.

The purpose of this letter is to issue our management decision regarding findings, if any, related to state or federal funds passed through the Texas Higher Education Coordinating Board that are noted in your organization's Appropriation Year 2021 Uniform Guidance 2 CFR Part 200 Subpart F Single Audit Report and related documentation.

Federal Fund Findings: None
State Fund Findings: None

We greatly appreciate the cooperation and assistance provided by your staff during our review. If you have any questions or comments, please contact Nancy Morales via email at Nancy.Morales@highered.texas.gov or call 512.427.6493.

Thank you for your assistance,

Mark Poehl CPA, CIA, CISA, CFE
Assistant Commissioner, Internal Audit and Compliance
512.427.6161
highered.texas.gov

THECB | Texas Higher Education COORDINATING BOARD

cc: Jason Mallory, Director of Internal Audit (jason.mallory@systems.tstc.edu)

cc: Carliss Hyde, Vice President, Sponsored Programs (carliss.hyde@tstc.edu)
cc: Cindy Reily, Associate Vice President, Office of Sponsored Programs (cmreily@tstc.edu)
cc: Lisa Frenette, Associate Vice President (lisa.frenette@tstc.edu)

Texas State Technical College
Internal Audit
Attestation Disclosures

Responsible Management	Issue Reported by Management	Report Date	Management's Corrective Action Plan	Internal Audit Assistance/Follow-up
			No new reports were made.	

The noted items were reported during the attestation process, and have been disclosed to the Chancellor. These were deemed to be worthy of disclosure to the Audit Committee.