

Meeting of the Board of Regents

Audit Committee

February 9, 2023
Waco, Texas



TABLE OF CONTENTS

Audit Committee

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

Minute Orders:

1. Status of Fiscal Year 2023 Audit Schedule & Other Projects..... A-1
Jason D. Mallory

2. Summary of Audit Reports..... A-3
Jason D. Mallory

3. Follow-up Schedule & Status A-5
Jason D. Mallory

4. Audit of HEERF III Grant as part of the American Rescue Plan (23-007A)..... A-11
Jason D. Mallory

5. Internal Network Penetration Test (EWCHEC) (23-009A) A-16
Jason D. Mallory

6. Internal Network Penetration Test (Waco Campus) (23-011A)..... A-22
Jason D. Mallory

7. Quarterly Results of Personal Property Verification Audit (23-003A)..... A-28
Jason D. Mallory

8. TAC 202 Compliance – Quarterly Update..... A-32
Jason D. Mallory

9. Attestation Disclosures A-36
Jason D. Mallory



**Texas State Technical College
Internal Audit
Status of Fiscal Year 2023 Audit Schedule & Other Projects**

Description	Division/Campus	Status	Project No.	Report Date	Last Audit Date	Audit Reason
INTERNAL AUDITS						
Internal Network Penetration Test	OIT/Harlingen Campus	Complete	23-004A	9/30/22	12/13/19	Risk Based
American Rescue Plan Act – Higher Education Emergency Relief Fund III	Office of Sponsored Programs, Student Services	Complete	23-007A	12/9/22	12/20/21	Risk Based
Internal Network Penetration Test	OIT/East Williamson County Campus	Complete	23-009A	12/9/22	9/27/19	Risk Based
Internal Network Penetration Test	OIT/Waco Campus	Complete	23-011A	12/9/22	3/10/20	Risk Based
Personal Property Verification Audit	Finance/College-wide	In Progress	23-003A	10/3/2022, 12/16/22	10/3/22	Risk Based
TAC 202 Follow-up Audit	OIT	In Progress	22-009A	11/10/2022, 1/13/2023	11/10/22	Required Bi-annually
Sick Leave Administration	HR	In Progress			-	Risk Based
T-Drive Audit	OIT/Several Departments	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
Audit of General IT Controls	OIT				6/28/17	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

<p>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.</p>	<p>Enrollment Services</p>	<p>Complete</p>	<p>23-0061</p>	<p>9/16/22</p>
<p>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: Determined the student did create repeated distractions for faculty and staff until he was expelled. Found opportunities to improve processes.</p>	<p>Student Discipline</p>	<p>Pending Management Responses</p>	<p>23-0101</p>	

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)	Res.p. Sr Mgr	Expect. Complete Date
Audit of HEERF III Grant as part of the American Rescue Plan (23-007A)	1.	No material exceptions identified.			

Internal Network Penetration Test (23-009A) (EWCHEC)	1. One employee should be required to complete the enhanced cybersecurity training provided by OIT since she provided us her credentials during our social engineering attempt. The other 3 who failed to complete their annual essentials training, which included cybersecurity, should be required to completed that.	Of 45 people subjected to our social engineering attempts, only 1 provided her Workday credentials. This employee works remotely. 3 employees failed to completed the required cybersecurity training.	1.1 Enhanced and essentials training will be completed.	Lissa Adams, Larry Mckee	2/28/23
---	--	--	---	--------------------------	---------

Internal Network Penetration Test (23-011A) (Waco)	1. There are opportunities to improve security awareness and procedures.	5 employees provided Workday credentials, 4 employees failed to complete essentials training, 1 employee left her computer unlocked, and 2 buildings were unlocked after hours.	1.1 All employees will be required to complete enhanced or essentials training. 1.2 Employees were reminded to lock doors after hours. Police will continue checking doors.	Elaine Sulak, Larry Mckee	1.1 2/28/23, 1.2 Complete
---	--	---	---	---------------------------	------------------------------

Report Name & No.	Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
Quarterly Results of Personal Property Verification Audit (23-003A)	1.	4,688 of 8,101 sample of assets verified as 12/16/22. 3,413 remaining on mainly the West Texas, Ft. Bend, and Harlingen campuses.			

TAC 202 Compliance – Quarterly Update (23-002A)	1.	5 more controls were identified as being implemented. Only 1 control left to implement from the original set of audits.			
---	----	---	--	--	--



**Texas State Technical College
Internal Audit
Follow Up Schedule & Status**

Completion Summary			
	9/30/22	12/31/22	Audits cleared from (Added to) Schedule
Audits from FY 2018	1	1	0
Audits from FY 2020	1	1	0
Audits from FY 2021	2	2	0
Audits from FY 2022	6	4	2
Audits from FY 2023	1	2	(1)
Net Total	11	10	1

Highlights:

TAC 202 Audits: 5 more controls were implemented.
Internal Network Penetration Test (23-004A): The marketing campaign to raise awareness of cyber threats was implemented.
Fixed Assets: All corrective actions required by the SAO in their 2021 financial processes audit were implemented. With over 50% of testing complete on the ongoing Fixed Asset audit, the results support that corrective action has been taken.
Academic Records Management Audit (22-005A): Final corrective action has been implemented.

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
<p>TAC \$202 Compliance Audits 22-022A, McKee, Scherwitz</p>	<p>1. Several required controls were not yet implemented.</p>	<p>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.</p>	<p>Ongoing: At 1/9/23, 11 systems and the IT general controls have been audited. A total of 0 general controls and 1 (total for all systems audited) application controls were not yet implemented. In this quarter, 5 controls were improved to implemented status.</p>		<p>Ongoing</p>
<p>PCI Compliance Audit (18-009A), Semien</p>	<p>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.</p>	<p>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.</p>	<p>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.</p>		<p>Ongoing</p>

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), 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 1/2/23: We are still working with L3 on a new lease that would include the Boneyard area. Currently waiting on a Survey of the areas L3 uses to be completed, before proceeding with a new lease. Hope to have new lease to present to L3 by the end of February, but this will depend on the completion of the survey.		5/31/23

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.	Pending Review: On 10/4/22, determined there were 141 accounts valued at \$90K still on the books. Accounting will research and close after year end accounting work is complete.		12/31/22
--	---	--	--	--	----------

Report Name & No., Resp. Sr Mgr Faculty	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
Credentials Audit (21-018A), Logan	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

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.	Partially Complete: 12/12/22 Jan Harvey met with OIT to form a plan for change management of tuition rate and program tier changes. Jan will continue to update rate changes and program tiers. A different employee will test the changes. This employee will not have access to modify tuition rates or program tiers. Changes and testing will be done in the test environment first. Additionally, a log has been created to document all changes and testing. Will test when fully implemented.		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
<p>Audit of Online Learning (22-002A), Cano-Montreal</p>	<p>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).</p>	<p>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.</p>	<p>Ongoing: 1/5/23 Will revisit next quarter, or when SOS has been approved and implemented.</p>	<p>SOS E.S. 2.20 currently has edits and is going through the a new SOS template process for policy revisions.</p>	<p>8/31/22</p>

<p>Career Services – Phishing Scam (22-039I), Darnell</p>	<p>1. Staff were manipulated into forwarding a fraudulent job posting to several students.</p>	<p>1.1 One employee is designated as the primary contact and approved 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.</p>	<p>Completed during audit. Internal Audit will test understanding through social engineering attacks.</p>	<p>8/1/22</p>
--	--	--	--	---------------

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
Internal Network Penetration Test (23-009A) - EWCHEC, Adams, McKee	1. One employee should be required to complete the enhanced cybersecurity training provided by OIT since she provided us her credentials during our social engineering attempt. The other 3 who failed to complete their annual essentials training, which included cybersecurity, should be required to completed that.	1.1 All training will be completed by February 28, 2023.	Ongoing		2/28/23
Internal Network Penetration Test (23-011A) - Waco, Sulak, McKee	1. There are opportunities to improve security awareness and procedures.	1.1 All employees who failed will be contacted by the Provost and HR to inform them. They will be required to take enhanced either the essentials or enhanced cybersecurity training. 1.2 All employees will be reminded to lock buildings after hours, and police will continue to randomly check doors.	Ongoing		2/28/23
			Completed in December 2022		Complete



Internal Audit Department

Audit Report

**Audit of HEERF III Grant as part of the American Rescue Plan (23-007A)
TEXAS STATE TECHNICAL COLLEGE**

December 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

We recently completed an audit of the Higher Education Emergency Relief Fund III (HEERF III/CARES 3) grant received from the Department of Education (ED) as a result of the American Rescue Plan (ARP) signed into law in March 2021. ARP provided \$39.6 billion in support to institutions of higher education with the intent to serve students and ensure learning continues during the COVID-19 pandemic. TSTC (College) was awarded \$37,633,773, of which \$18,938,740 was allocated for students and \$18,695,033 for the institution. In this audit we refer to this money as CARES 3. The College also received an additional \$1,945,979 due to being a Minority Serving Institution.

These funds are in addition to the previous Coronavirus Aid, Relief and Economic Security Act (CARES Act) and Coronavirus Response and Relief Supplemental Appropriations Act (CRRSAA) grants. In total, the College has received approximately \$68.9 million for all three installments of CARES funds and a total of \$3.7 million as a Minority Serving Institution. Only the third installment of CARES 3 funds were reviewed in this audit.

The primary objective of this audit was to ensure the awarding, disbursement, timing, and reporting of the CARES 3 funds complied to the ARP, and other specific rules and available guidance. Similar to previous the other two CARES audits, we verified the processes and internal controls relied upon in the awarding, disbursing, timing and reporting of awards. We accomplished our objectives by testing a sample of awards made to students during fiscal year 2022, as well as tested a sample of expenditures made by the College using the funds in that same time period.

We determined the use of CARES 3 funds generally complied with applicable rules. We found a few isolated instances of discrepancies in the student portion of the awards; however, we would not characterize any of these as significant non-compliance matters. Management was made aware of our observations.

Introduction

The objective of the CARES funds was to assist institutions of higher education with preventing, preparing for, and responding to the Coronavirus. This money was intended to assist both students and the College.

Student Portion

To qualify for assistance, students with exceptional need were prioritized; several requirements implemented for CARES 1 were no longer required for CARES 2 or CARES 3. Students could use funds for any component of their cost of attendance or for emergency costs that arose due to coronavirus, including tuition, food, housing, health care or child care. The College utilized an awarding protocol to identify students' needs to help distribute the funds. To apply, students submitted a request through Progress Pathway which feeds directly to Salesforce, a customer relationship management software that allows the College to track, document and communicate with the student. Once an application was submitted, an Advocacy and Resource Center (ARC)

representative within Retention Services was assigned to the student’s case and contacted each student. ARC representatives made the final determination on the amount of each award based on those applications and discussions with the student. The Financial Aid and Student Accounting Departments processed and disbursed the approved awards, respectively. Students were able to receive a maximum amount of \$6,000 per academic/fiscal year; funds awarded for tuition and fees did not apply to this maximum amount. Additionally, students could receive awards specifically for tuition and/or for any other component of their cost of attendance.

As of November 30, 2022, \$18,542,797.05 of CARES 3 for students had been disbursed. Of this amount, \$10,120,618 was directly applied to tuition and fees, known as CARE-T, with 3,388 unduplicated (4,829 duplicated) students receiving an average award of \$2,987. The following table details the amounts of CARE-T awards by each campus.

CARE-T (tuition assistance, unduplicated students)

Campus	Amount	% of Total	# of Students	% of Total Students
Waco	\$2,377,895	23.50%	673	19.86%
EWCHEC	\$289,546	2.86%	94	2.77%
Harlingen	\$2,029,648	20.05%	849	25.06%
Fort Bend	\$1,005,348	9.93%	268	7.91%
Sweetwater	\$492,406	4.87%	155	4.57%
Abilene	\$370,494	3.66%	94	2.77%
Brownwood	\$10,791	0.11%	3	0.09%
Breckenridge	\$69,301	0.68%	28	0.83%
Marshall	\$762,452	7.53%	207	6.11%
North Texas	\$537,070	5.31%	129	3.81%
Online Programs	\$2,175,667	21.50%	888	26.21%
Total	\$10,120,618	100%	3,388	100%

The remaining \$8,422,179.05 was awarded for other cost of attendance components such as child care, rent and school supplies, known as CARE-3, with 3,817 unduplicated (5,881 duplicated) students receiving an average award of \$2,206. The following table details these awards by each campus.

CARE-3 (non-tuition assistance, unduplicated students)

Campus	Amount	% of Total	# of Students	% of Total Students
Waco	\$1,949,907	23.15%	883	23.13%
EWCHEC	\$50,597	0.60%	33	0.83%
Harlingen	\$2,934,648	34.84%	1,345	35.24%
Fort Bend	\$356,587	4.23%	213	5.58%
Sweetwater	\$446,015	5.30%	183	4.79%
Abilene	\$199,483	2.37%	107	2.80%

Brownwood	\$22,243	0.26%	17	0.45%
Breckenridge	\$43,588	0.52%	26	0.68%
Marshall	\$1,016,501	12.07%	353	9.25%
North Texas	\$121,956	1.45%	63	1.65%
Online Programs	\$1,280,654	15.21%	594	15.56%
Total	\$8,422,179	100%	3,817	100%

Institutional Portion

A documented plan for distributing the institutional funds was put in place during the first installment of CARES funds. Institutional funds could cover any costs associated with significant changes to the delivery of instruction as a result of the Coronavirus, including lost revenue, reimbursement for expenses already incurred, technology costs associated with a transition to distance education, faculty and staff trainings and payroll. Funding contractors for the provision of pre-enrollment recruitment activities, marketing or recruitment, endowments or capital outlays associated with facilities related to athletics, sectarian instruction or religious worship were not allowable. The Office of Sponsored Programs helped ensure the use of these funds were both authorized and allowable.

Institutional funds are not categorized by each installment received, like the student portion. Rather, all CARES institutional installments are grouped together with each installment being added as a running total. All three CARES institutional installments totaled \$39,987,345. As of November 30, \$37,900,876 of the total institutional funds received were spent. The majority of funds were used by the Instructional division, which included enhancements to their innovation, modality, upskilling and job pathways and growth capacity initiatives. Other funds were allocated to Student Services, OIT and Physical Plant. Purchases included safety and cleaning supplies, additional lab equipment so students could meet social distancing requirements, and an expansion of online learning.

As of the date of this report, the deadline to disburse all CARES 3 funds was extended to June 30, 2023. Internal Audit worked closely with members of Sponsored Programs, Financial Aid, Retention Services, Student Learning and Procurement to perform this audit.

Objectives

The primary objective of this audit was to ensure the awarding, disbursement, timing, and reporting of the CARES 3 funds complied to the ARP and other specific rules and available guidance. Internal controls relied upon to ensure compliance were also validated.

Scope & Methodology

The scope of our audit included all student & institutional disbursements during fiscal year 2022. To accomplish our objectives, we selected a sample of student and institutional awards and verified the uses were appropriate. For students, we validated that a process was in place and being

followed, that award amounts were approved, and that documentation from the student was obtained if the award was applied to their outstanding account balance. We reviewed approval controls and reporting requirements. We utilized the following guidance as our methodology.

- Department of Education: American Rescue Plan (HEERF III)
- Department of Education HEERF III FAQ's
- Department of Education HEERF III Fact Sheet
- HEERF III Reference Page

General Observations

Since March 2020, over \$37.9 million in institutional funds have been disbursed with the assistance and coordination of multiple departments. Similarly, over \$28.5 million allocated for students has been awarded. With each installment of funds, Student Services continued to improve their awarding protocols and documentation efforts. We commend them for contacting students who applied for funds and assisting them quickly, while also offering additional external resources that might assist them as well. In the initial CARES audit we identified related party awards. We did not identify any in the previous CARES 2 audit. In an effort to reduce this risk even more, employees were ineligible to receive CARES funds beginning August 2021.

For institutional funds, the same request process established with CARES 1 &2 was performed. Specifically, for instructional funds, requests included detailed documentation and approval.

Summary of Findings

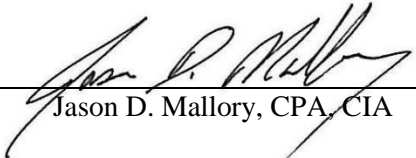
No material exceptions were identified.

Opinion

Based on the audit work performed, the College complied with requirements surrounding the American Rescue Plan other guidance associated with the CARES 3 funds. Student and institutional disbursements were used for allowable purposes, and reporting requirements are being properly performed.

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

December 9, 2022

Date



Internal Audit Department

Audit Report

Internal Network Penetration Test (23-009A)
TEXAS STATE TECHNICAL COLLEGE
East Williamson County Campus

December 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

Between October 24, 2022 and November 11, 2022 we performed vulnerability scans and penetration testing of the College's internal network on the East Williamson County 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 this 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.

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 2 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.

We determined that employees do not expose sensitive information by disposing of documents in recycle/trash bins or leaving them in public view. Computer desktops and offices are inaccessible. Wireless networks are appropriately segregated, and protected by secured logon protocols and encryption. We were unable to access any restricted information on the network. Usable wireless access is only available from inside the building, open ports are disconnected from the network, and security personnel actively monitor the facility. Facilities were locked during non-business hours. Finally, IT related closets are restricted by locks that require both a physical key and badge swipe.

We were successful in social engineering only one employee. This is a notable improvement over the last test conducted in fiscal year 2020. We also identified 3 employees who did not complete their required cybersecurity training.

Introduction

The East Williamson County Campus in Hutto is shared by TSTC, Temple College (TC), and other colleges. In an operating agreement signed by both parties in July of 2011, TC agreed to provide all utilities, custodial services, grounds keeping, IT costs, and routine maintenance of the facility. This includes all IT operations and network activities, including telephone services. TSTC maintains its own instructional equipment and any other property it uses for its sole instructional benefit. To that end, the OIT Department of TSTC maintains all College owned computers, printers, desktops and other similar equipment, and provides help desk services to TSTC staff and students who require assistance with logging into their TSTC related accounts or accessing computers in the lab. The TC IT department provides help desk services for telephone and network related issues.

Because IT services are primarily provided by TC, our testing focused on processes, services, and activities that presented risks to TSTC. The Office of Information Technology provided a map detailing all areas primarily occupied by the College.

To ensure the integrity of the results, we only notified the Provost, select managers and members of the Office of Information Technology of our test work. The specifics and timing of our tests were not disclosed to anyone in an attempt to make this test as realistic as possible to achieve reliable results.

This test verified not only physical and logical controls related to safety and security and IT security, it also validated human behavior and training in certain regards.

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 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 46 employees who have access to sensitive information. We scanned network services, attempted to access areas that should be restricted, tested open ports and reviewed available training documentation.

General Observations

Even though we increased the number of employees we attempted to social engineer, all but one rejected our attempts. There were no “repeat offenders” from our last test. Additionally, reports to the TSTC Help Desk regarding our suspicious emails and telephone calls increased substantially since that previous test. This is a good indicator that employees recognized the emails and telephone calls as suspicious.

Wired and wireless networks are segregated between privileged and guest accounts, with services being appropriate on each. Wireless access points do not emit signals that can be used by bad actors outside of the physical perimeters of the originating building. We did not locate any open ports that allowed us to perform network scans. Access to closets containing networking equipment were kept locked during and after business hours. Access to faculty offices were kept restricted from unauthorized users by locked doors during and after business hours. Security personnel made their presence known by consistently surveying the campus floors at all hours of the day. In fact, they made our tests difficult. Access to computer lab desktops were restricted by requiring the use of a student name and ID in order to logon.

Summary of Finding

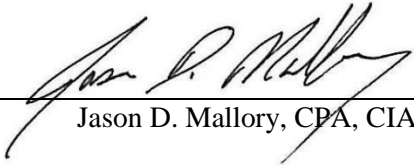
One employee should be required to complete the enhanced cybersecurity training provided by OIT since she provided us her credentials during our social engineering attempt. The other 3 who failed to complete their annual essentials training, which included cybersecurity, should be required to complete that.

Opinion

Based on the audit work performed, IT assets and information are well protected on the East Williamson County Campus. The deficiencies we noted appear to be isolated issues with individual employees rather than a systemic issue on the campus.

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

December 9, 2022

Date

AUDIT FINDING DETAIL

Finding #1: One employee should be required to complete the enhanced cybersecurity training provided by OIT since she provided us her credentials during our social engineering attempt. The other 3 who failed to complete their annual essentials training, which included cybersecurity, should be required to complete that.

Criterion: We made telephone calls and sent emails to 45 employees on the East Williamson County Campus in attempt to steal their Workday user ID and password. We also reviewed the training records of campus employees to ensure they completed required cyber security training.

Of 45 people subjected to our social engineering attempts, only 1 provided her Workday credentials. This employee works remotely.

Of the 45 employees tested, 3 failed to complete the required cybersecurity training.

Consequences: Increased risk of inappropriate access to sensitive data.

Possible Solutions: We recommend the specific employee who provided their login credentials be required to complete enhanced cybersecurity training. For the other 3, we recommend they be required to complete their annual essentials training. All should be counseled about their actions.

Management Response

Management on the East Williamson County Campus agrees with the observations made in the audit. One employee who reports to another manager provided information to a social engineering email that she should have disregarded. Three other employees failed to complete their annual essentials training. Lissa Adams, Provost, with assistance from Kelly Contella, Sr. Executive Manager in HR, will contact each employee and/or their managers to inform them of the test results. The employee who was compromised will be required to take cybersecurity training taught by Scott Hodkinson in IT Risk Management when he offers the next round of training in February 2023. The other employees will be required to complete their essentials training that they failed to complete several months ago. Notification and counseling will take place immediately with all these employees. All training will be completed no later than February 28, 2023. Lissa Adams will be responsible for implementation of this corrective action plan.



Internal Audit Department

Audit Report

Internal Network Penetration Test (23-011A)
TEXAS STATE TECHNICAL COLLEGE
Waco Campus

December 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

Between October 24, 2022 and November 11, 2022 we performed vulnerability scans and penetration testing of the College's internal network on the Waco 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 this 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.

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 2 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.

We determined that employees do not expose sensitive information by disposing of documents in recycle/trash bins or leaving them in public view. Computer desktops and offices are generally inaccessible. Wireless networks are appropriately segregated, and protected by secured logon protocols and encryption. We were unable to access any restricted information on the network. Usable wireless access is only available from inside the building, open ports are disconnected from the network. Finally, IT related closets and rooms are restricted by locks that require both a physical key and badge swipe.

We were successful, however, in social engineering 5 employees and gained access to 1 unlocked computer when the employee stepped away. We identified 4 instances of employees not completing required cybersecurity training. Finally, there were 2 buildings left unlocked after business hours.

Introduction

College headquarters are located on the Waco Campus, and it serves as a network hub for all other campuses by housing all critical information systems. The Office of Information Technology (OIT) Division 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. All employees have a role in ensuring assets and data are protected.

To ensure the integrity of the results, we only notified the Provost, select managers and members of the Office of Information Technology of our test work. The specifics and exact timing of our tests were not disclosed to anyone in an attempt to make this test as realistic as possible to achieve reliable results.

This test verified not only physical and logical controls related to safety and security and IT security, it also validated human behavior and training in certain regards.

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 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 114 employees who have access to sensitive information. We scanned network services, attempted to access areas that should be restricted, tested open ports and reviewed available training documentation.

General Observations

Even though we increased the number of employees we attempted to social engineer, all but 5 rejected our attempts. There were no “repeat offenders” from our last test. Additionally, reports to the TSTC Help Desk regarding our suspicious emails and telephone calls increased substantially since that previous test. This is a good indicator that employees recognized the emails and telephone calls as suspicious.

Wired and wireless networks are segregated between privileged and guest accounts, with services being appropriate on each. Wireless access points do not emit signals that can be used by bad actors outside of the physical perimeters of the originating building. We did not locate any open ports that allowed us to perform network scans. Access to closets containing networking equipment were kept locked during and after business hours. Access to faculty offices were kept restricted from unauthorized users by locked doors during and after business hours. Access to computer lab desktops were restricted by requiring the use of a student name and ID in order to logon.

Summary of Finding

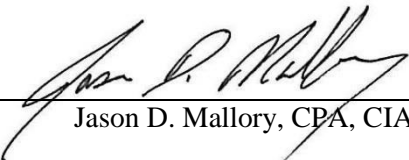
There are opportunities to improve security awareness and procedures.

Opinion

Based on the audit work performed, IT assets and information are well protected on the Waco Campus, but there is a need to improve awareness and other security related procedures.

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

December 9, 2022

Date

AUDIT FINDING DETAIL

Finding #1: There are opportunities to improve security awareness and procedures.

Criterion: We made telephone calls and sent emails to 114 employees on the Waco Campus in attempt to steal their Workday user ID and password. We also reviewed the training records of these same employees to ensure they completed required cyber security training. We attempted to access personal computers when employees stepped away. We scanned campus networks looking for vulnerabilities. And, we attempted to access campus buildings after business hours.

- Five employees provided Workday logon credentials in response to our social engineering test.
- Four employees failed to completed the annually required cybersecurity training.
- One employee in the library left her computer unlocked when she stepped away. We were able to get on that computer. Her email was accessible, as were other programs.
- The ITC and Provence Center had doors that were unlocked after 8 PM. We did not enter the buildings, but there was no evidence anyone was in the buildings. We immediately informed the Police so that they could lock the doors.

Consequences: Increased risk of inappropriate access to sensitive data.

Possible Solutions: We recommend the specific employees who provided their logon credentials or left her computer unlocked be required to complete enhanced cybersecurity training. For the ones who failed to complete their annual essentials training, we recommend they be required to now complete it. We also recommend each employee be made aware of their actions.

For the buildings, we recommend the campus community be reminded to lock all external doors to facilities after hours, with a more thorough check being conducted by the Police.

Management Response

Management on the Waco Campus agrees with the observations made in the audit. Five employees who report to other managers provided information to social engineering emails and telephone calls that they should have disregarded. Four other employees failed to complete their annual essentials training. And, one employee failed to lock her computer when she stepped away. Elaine Sulak, Associate Provost, with assistance from Kelly Contella, Sr. Executive Manager in HR, will contact each employee and/or their managers to inform them of the test results. The 5 employees who were compromised and the 1 who failed to lock her computer will be required to take cybersecurity training taught by Scott Hodkinson in IT Risk Management when he offers the next round of training in February 2023. The other 4 employees will be required to complete their essentials training that they failed to complete several months ago. Notification and counseling will take place immediately with all these employees. All training will be completed no later than

February 28, 2023. Elaine Sulak will be responsible for implementation of this corrective action plan.

Regarding the unlocked buildings, employees in the 2 buildings that were found unlocked will be reminded by Elaine Sulak to lock all doors after hours. Campus Police will continue to randomly check doors after hours. A campus-wide reminder to lock doors after hours will be made in the next Provost update. Because most administrative staff in the Provence building work in hybrid mode, there is not a designated person to lock doors. IT staff are generally in it on a consistent basis, so they will be asked to check all doors when they leave for the evening. Elaine Sulak, Associate Provost, will be responsible for ensuring these reminders are made no later than December 16, 2022.



To: Audit Committee
From: Jason D. Mallory, Audit Director 
Subject: Quarterly Results of Personal Property Verification Audit (23-003A)
Date: December 16, 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.

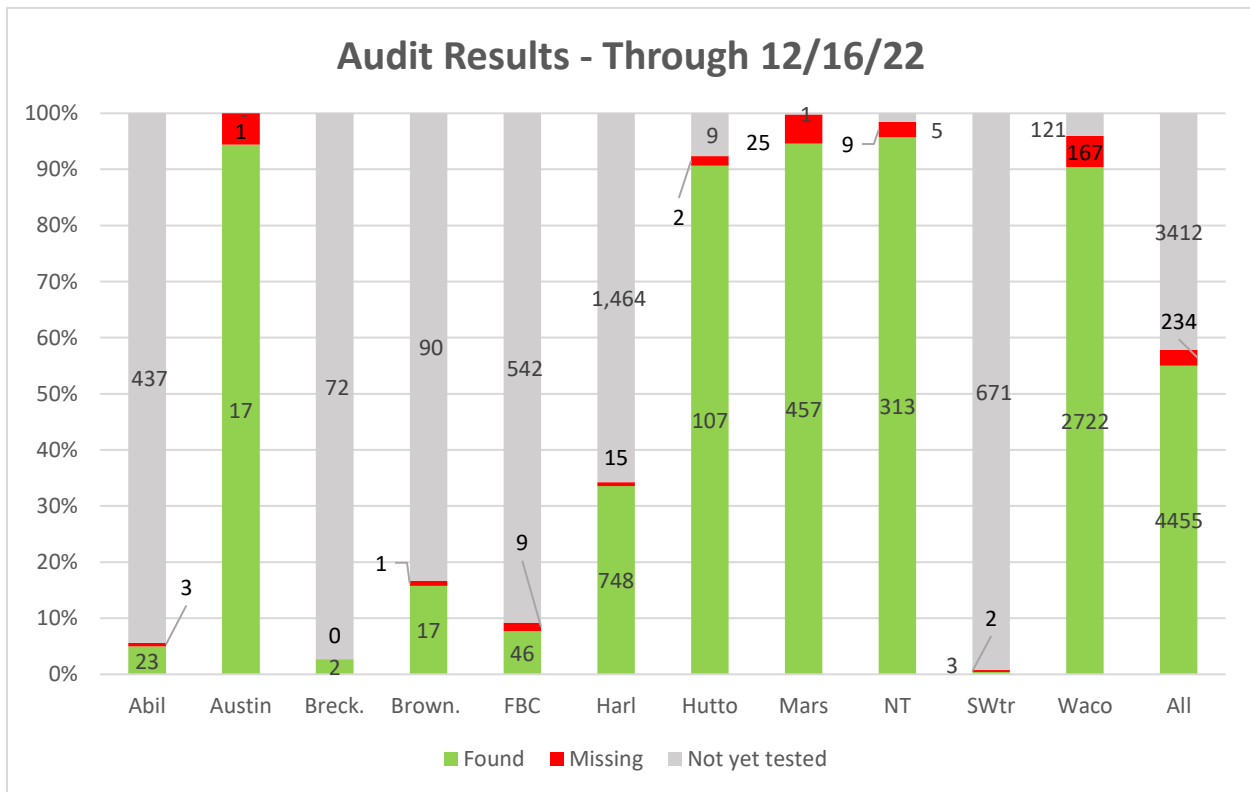
The "SPA Process User's Guide" also provides specific guidance on select internal controls, such as the annual inventory of personal property. This guidance, though, seems more aimed at users of the Comptroller's asset accounting system. The Code exempts the College from using that system, so certain 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

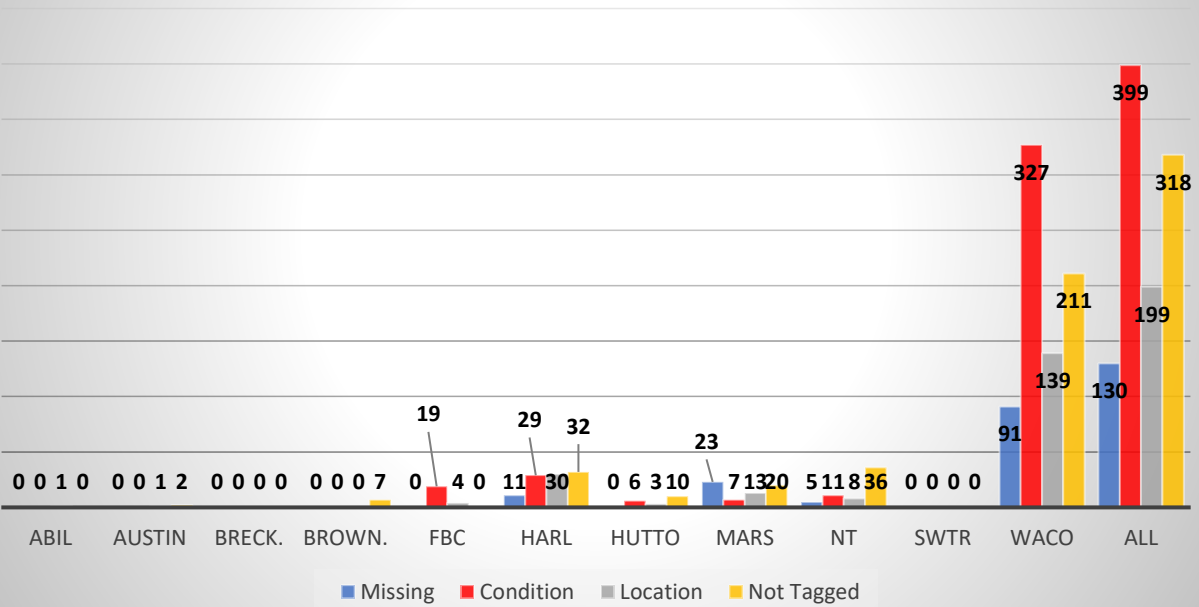
test results for easy follow-up with stewards as we identify discrepancies. The following are the results of our tests as of December 16, 2022:

Campus	Total	Sample	Tested	Left to Test	% Left to Test
Abilene	1,172	463	26	437	94%
Austin	19	18	18	0	0%
Breckenridge	183	74	2	72	97%
Brownwood	385	108	18	90	83%
Ft. Bend	1,864	597	54	543	91%
Harlingen	6,675	2,227	763	1,464	66%
EWCHEC	445	118	109	9	8%
Marshall	1,478	483	482	1	0%
North Texas	923	327	322	5	2%
Sweetwater	2,045	676	5	671	99%
Waco	9,259	3,010	2,889	121	4%
ALL	24,448 ^{Note 1}	8,101	4,688	3,413	42%

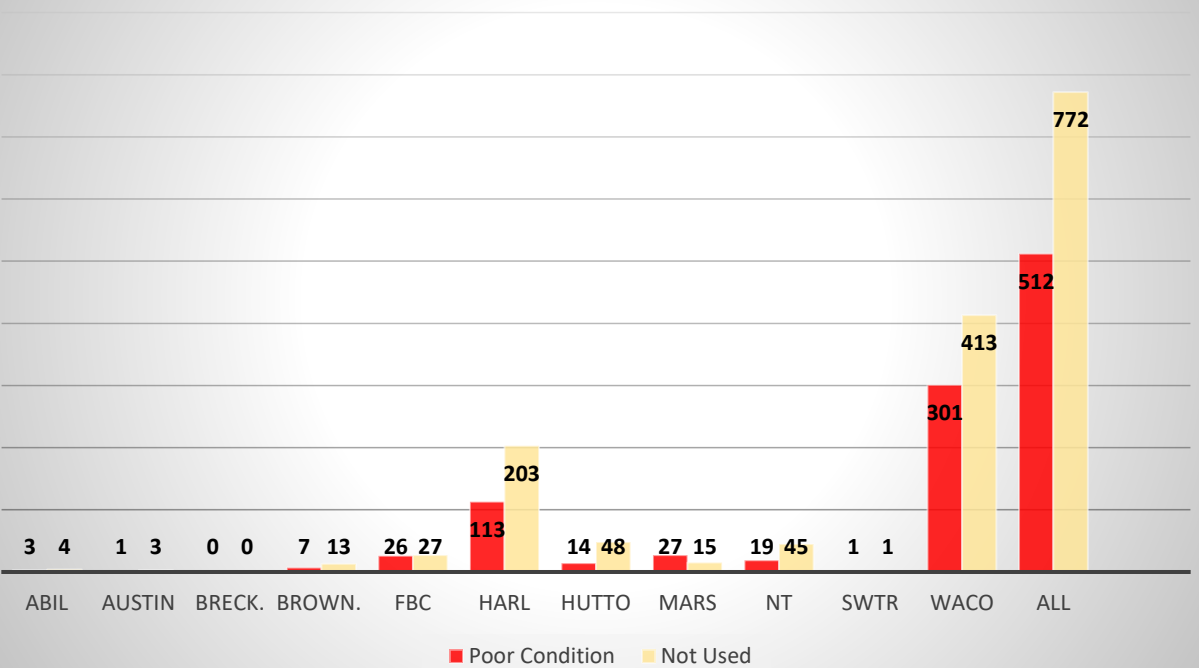
Note 1: This was the total number of assets on 8/7/22 when our sample was selected. This number fluctuates daily due to purchases and disposals, but has consistently remained between 24 and 25 thousand.



Recording & Tag Exceptions



Possible Opportunities for Disposal



Of the 1,429 asset stewards on record as of the date of this report, 1,191, or 83% 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 for stewards on record when inventory was taken was 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
Chad Wooten, Interim 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

February 2023

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.





To: Audit Committee
 From: Jason D. Mallory, Audit Director
 Subject: TAC 202 Compliance – Quarterly Update
 Date: January 13, 2023

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 October 1 through December 31, 2022, 5 more required control were implemented for the Canvas 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
As of September 2022	50	0	0	2	52

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

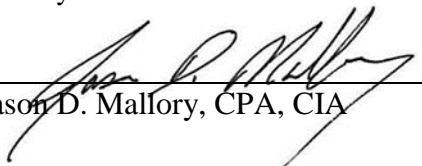
Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
Oct 2022 – Dec 2022	43	10	0	0	53
July 2022 – Sept 2022	38	10	5	0	53
Difference	+5	0	-5	0	

TWC Server

Original Audit: May 16, 2022

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
Oct 2022 – Dec 2022	46	4	1	0	51
July 2022 – Sept 2022	46	4	1	0	51
Difference	0	0	0	0	

Submitted by:



Jason D. Mallory, CPA, CIA

January 13, 2023
Date

- cc: Mike Reeser, Chancellor/CEO
Gail Lawrence, Deputy Chancellor
Jennifer Tindell, Chief of Staff
Shelli Scherwitz, Executive Vice President/OIT
Larry McKee, Executive Director/OIT Compliance



Texas State Technical College
Internal Audit
Attestation Disclosures

Responsible	Issue Reported by Management	Report Date	Management's Corrective Action Plan	Internal Audit Assistance/Follow-up
EVC/COO	We became aware of a potential impropriety that we disclosed to Internal Audit. A deeper understanding of what actually occurred will take place on January 23rd. By way of our conversation with Jason and this email we are documenting the disclosure so that his team can review the matter.	1/5/23	Pending further information.	Internal Audit will gain a better understanding in the near future of the concern and offer an opinion and recommendations, if applicable.

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.