

Meeting of the Board of Regents

Audit Committee

August 8, 2024

Waco, Texas



**Audit Committee Meeting
of the Board of Regents**

John B. Connally Administration & Visitor Center
1651 E. Crest Dr., Waco, TX, 76705*

Thursday, August 8, 2024
9:30 a.m.

AGENDA

[Lizzy de la Garza Putegnat (Chair), Robb Misso]

**I. MEETING CALLED TO ORDER BY AUDIT COMMITTEE CHAIR LIZZY DE LA GARZA
PUTEGNAT**

II. COMMITTEE CHAIR COMMENTS

III. MINUTE ORDERS & REPORTS

1. Proposed Audit Plan for Fiscal Year 2025	<i>Jason D. Mallory</i>	A-1
2. Status of Fiscal Year 2024 Audit Schedule & Other Projects	<i>Jason D. Mallory</i>	A-7
3. Status of Construction Audits	<i>Jason D. Mallory</i>	A-13
4. Summary of Audit Reports	<i>Jason D. Mallory</i>	A-14
5. Follow-up Schedule & Status	<i>Jason D. Mallory</i>	A-17
6. Procurement Card Program Audit (24-018A)	<i>Jason D. Mallory</i>	A-24
7. CRIMES Software Audit (24-019A)	<i>Jason D. Mallory</i>	A-30
8. Internal Network Penetration Test (24-024A)	<i>Jason D. Mallory</i>	A-36
9. Quality Assurance Review of Internal Audit	<i>Jason D. Mallory</i>	A-42

**Presiding officer will be physically present at this address.*

(c) denotes Consent Agenda Item

10. Student Grievances Audit (24-022A)	<i>Jason D. Mallory</i>	A-47
11. TAC 202 Compliance – Quarterly Update	<i>Jason D. Mallory</i>	A-50
12. FY 2023 Single Audit Evaluation Management Letter	<i>THECB</i>	A-54
13. Attestation Disclosures	<i>Jason D. Mallory</i>	A-55
IV. CHANCELLOR COMMENTS		
V. BOARD COMMENTS		
VI. ADJOURN		

**Presiding officer will be physically present at this address.*

(c) denotes Consent Agenda Item



Board Meeting Date: August 8, 2024 **Proposed Minute Order #:** IA 01-24 (c)

Proposed By: Jason D. Mallory, Director of Audits

Subject: Proposed Audit Plan for Fiscal Year 2025

Background: The Texas Internal Auditing Act, Chapter 2102 of the Texas Government Code, requires Board of Regents' approval for the annual audit plan and any revisions.

Justification: The guidelines of the Internal Auditing Act require that the internal auditor use risk assessment techniques to prepare an annual audit plan. The plan must identify the individual audits to be conducted during the year, and requires approval by the Board of Regents.

Additional Information: None

Fiscal Implications: Funds available as budgeted for fiscal year 2025.

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

Attachment(s): Proposed Audit Plan – Fiscal Year 2025

Recommended Minute Order: "The Texas State Technical College Board of Regents approves the audit plan for fiscal year 2025."

Recommended By: [ORIGINAL SIGNED BY]
Jason D. Mallory, Director of Audits



Fiscal Year 2025 Audit Plan

Proposed August 8, 2024



Executive Summary

The purpose of the Audit Plan (Plan) is to outline audits and other activities the Internal Audit Department will conduct throughout fiscal year 2025. The Plan was developed through collaboration with the Board of Regents, Executive Management, and managers who oversee the major processes and activities that are crucial to fulfilling the College’s mission. Internal Audit staff also provided input.

Documented assessments which considered the impact and likelihood of significant risks were performed on each major process and activity by the respective managers. The Internal Audit Department used the information provided by these risk assessments, as well as the other input provided, to assist in selecting the audits detailed in this proposal. We considered the following factors when selecting each audit:

- Time since last audit
- Risk or impact of fraud
- Financial impact a process, Department, or activity has on the College
- Turnover of key personnel
- Request by management or the Board
- Significance of regulatory exposure
- Recent known issues within a process, Department, or activity
- Regulatory requirement
- Recent changes to significant procedures/processes, or increased activity

The Plan, its development, and approval are intended to satisfy requirements under the College’s Internal Audit Charter (SOS GA.1.4) and the Texas Internal Auditing Act (TGC Chapter 2102).

The Plan includes 22 full-scope internal audits, 1 limited scope audit. Eight of the 22 full-scope audits will be continuations of construction audits started in fiscal year 2024. The Plan also anticipates follow-up audits, investigations, and consulting type of projects. The Plan includes compliance and operational audits, audits of information technology assets and resources (IT), audits required by regulation, and those specifically requested by Regents and/or Executive Management.

Internal Audit Available Time

Total hours (5 Staff * 2,080 available man hours)	10,400	100%
Less: Estimated holidays, leave & training	1,580	15%
Total hours available for audits, other projects & administration	8,820	85%

Proposed 2025 Audit Plan

Operational Audits

1. **TEC 51.9337 (Contracting) Audit:** Required to be audited annually. This audit will test compliance to TEC 51.9337 related to contracting. Some of the tests that will be performed include policy requirements, training, conflict of interest disclosures, tracking of contracts, approval authority, and the availability and compliance to a College contract handbook. Contract performance will also be tested.
2. **Outsourced Construction Audit(s):** The College is in the process of constructing several buildings throughout the State. Eight audits started in fiscal year 2024 will continue into 2025. An external firm who specializes in construction auditing is auditing contract compliance to identify cost recovery opportunities. Additional audits may be added.
3. **SB 17 Compliance Audit:** This audit will verify the College does not have any diversity, equity, or inclusion related processes, offices, or other requirements that are prohibited by Texas Education Code 51.3525.
4. **Audit of Federal Financial Audit Compliance:** This audit will test compliance to Title IV requirements that relate to Pell grants, student loans, and return of funds.
5. **Audit of the Student Discipline Process:** This audit will test the effectiveness and efficiency of disciplinary matters involving students.
6. **Audit of Workforce Development:** This audit will primarily test business-related processes within Workforce Development, such as purchases, travel, leave administration, and asset security. It may test select enrollment data for a sample of courses being taught, especially if funded by a grant.
7. **Audit of the Hiring Process:** This audit will test the effectiveness and efficiency of the hiring process, to include employee recruiting procedures, pre-screening steps (such as drug and background screening), and onboarding processes.
8. **Travel Expense Audit:** This audit will test recent travel expenses to identify unusual trends and wasteful spending.
9. **Tuition Audit:** This audit will test the calculation of tuition.
10. **Review of Syllabi:** This will be a limited scope review of course syllabi to ensure the information presented reflects actual course requirements and grading methodology.

11. **Clery Compliance Audit:** This audit will test compliance to the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act.

IT Audits

1. **Internal Network Penetration Test (North Texas campus):** This audit will test the security of sensitive information accessible through the College's network. It will also test manual procedures which safeguard sensitive information. Social engineering will be a key component in this project.
2. **Internal Network Penetration Test (Fort Bend campus):** This audit will test the security of sensitive information accessible through the College's network. It will also test manual procedures which safeguard sensitive information. Social engineering will be a key component in this project.
3. **Internal Network Penetration Test (New Braunfels campus):** This audit will test the security of sensitive information accessible through the College's network. It will also test manual procedures which safeguard sensitive information. Social engineering will be a key component in this project.
4. **Audit of IT security requirements in the contract with the Texas Workforce Commission:** This contract relates to information provided to the College for its funding formula. The contract requires and audit every 2 years to ensure required security provisions are in place.
5. **Workday Audit:** This audit will TAC 202 controls for Workday. These controls ensure the integrity, reliability, confidentiality, and availability of the system
6. **TAC 202 Follow-up:** This will be a quarterly follow-audit of TAC 202 controls that were found in prior audit to need improvement.

Other Projects

1. **Follow-ups on Past Audit Recommendations:** These will review the implementation status of corrective action plans on outstanding audit recommendations.
2. **Hotline Assessments and Investigations:** These will involve administering the anonymous ethics hotline, reviewing all reported complaints, and performing appropriate procedures to validate each complaint.
3. **Other projects:** Will include projects requested by management. Will also include the preparation of the Annual Audit Report and the 2025 Audit Plan.

4. **Audit Standards Update:** This project will include updating Internal Audit policies and procedures to match revised professional standards.



Texas State Technical College
Internal Audit
Status of Fiscal Year 2024 Audit Schedule & Other Projects

Description	Division/Campus	Status	Project No.	Report Date	Last Audit Date	Audit Reason
INTERNAL AUDITS						
Accounting Controls Audit	Foundation/Finance	Complete	24-001A	9/6/23	9/9/22	Risk Based
Public Funds Investment Act Compliance Audit	Finance	Complete	24-005A	11/10/23	9/24/21	Required every 2 years
Grant Audit	Office of Sponsored Programs	Complete	24-008A	12/4/23	-	Risk Based
Payment Card Industry (PCI) Audit	OIT	Complete	24-002A	2/12/24	5/14/18	Risk Based
Safety & Security Audit	Safety	Complete	24-007A	3/22/24	4/12/21	Risk Based
Procurement Cards Audit	Procurement	Complete	24-018A	5/14/24	2/22/11	Risk Based
CRIMES System TAC 202 Audit	Police/OIT	Complete	24-017A	5/23/24	-	Risk Based
Internal Network Penetration Test	Marshall Campus	Complete	24-024A	6/6/24	3/26/21	Risk Based
Internal/External Quality Assessment Review	Internal Audit	Complete	24-004A	6/14/24	7/15/21	Required every 3 years
Student Grievance Process Audit	Operations	Complete	24-022A	6/27/24	-	Risk Based
TAC 202 Follow-up Audit	OIT	Complete	24-009A	7/1/24	10/31/202, 12/31/2023, 3/31/2024	Required Bi-annually
Internal Network Penetration Test	West Texas Campuses	In Progress			12/14/20	Risk Based
Fleet Management Audit	Fleet	In Progress			5/11/11	Risk Based
TEC 51.9337 (Contracting) Audit	Contract Office	In Progress			5/18/23	Required Annually
Construction Audits	Facilities, Planning & Construction		24-006A			
JBC Remodel		In Progress			-	Risk Based
Waco Annex		In Progress			-	Risk Based

Description	Division/Campus	Status	Project No.	Report Date	Last Audit Date	Audit Reason
Abilene CCAP		In Progress			-	Risk Based
Waco CCAP		In Progress			-	Risk Based
Marshall CCAP		In Progress			-	Risk Based
Fort Bend CCAP		In Progress			-	Risk Based
EEC & TSC Renovation		In Progress				Risk Based
Harlingen CCAP		In Progress			-	Risk Based

EXTERNAL AUDITS

FMLA Investigation performed by the Department of Labor - determined the complaint by former employee had no merit.	HR	Complete		11/20/23		
Summary - State of Texas Financial Portion of the Statewide Single Audit Report for the Year Ended August 31, 2023 by the State Auditor's Office	Finance	Complete	SAO 24-555	2/22/24		
Summary - State of Texas Federal Portion of the Statewide Single Audit Report for the Year Ended August 31, 2023 by the State Auditor's Office	Finance	Complete	SAO 24-316	2/22/24		
Summary - Report on Full-time Equivalent State Employees for Fiscal Year 2023 by the State Auditor's Office	HR	Complete	SAO 24-703	2/22/24		
FY 2023 Single Audit Evaluation Management Letter by the THECB	Finance	Complete		6/17/24		
Post Payment Audit performed by the Comptroller's Office	Procurement, Accounting	In Progress				
Investigation by the State Auditor's Office related to a specific vendor.		In Progress				

OTHER INTERNAL PROJECTS

Description	Division/Campus	Status	Project No.	Report Date	Last Audit Date	Audit Reason
Internal Hotline: Received an anonymous concern of potential illegal drug use in a dorm. Results: The report was forwarded to housing personnel and the police for review and resolution. As of 12/11/2023, drug use has not been observed.	Housing - Waco	Complete	24-016I	N/A		
Internal Hotline: Received an anonymous concern from a parent complaining about being required to purchase a meal plan Results: The report was forwarded to Campus Services to consider whether there opportunities to improve meal plan guidelines. IA considered this a management matter, and not representative of fraud, waste, and abuse.	Campus Services	Complete	24-011I	N/A		
Internal Hotline: Received an anonymous report of an instructional designer having a second job. There were no details regarding conflict of time, misuse of equipment, etc. Results: This was forwarded to the AVC - Instructional Shared Services. The instructional designer completed a conflict of interest disclosure that will be considered by the COI committee. His supervisors do not feel he has a conflict, but the COI committee will make the	Operations	Complete	24-010I	12/20/23		

Description	Division/Campus	Status	Project No.	Report Date	Last Audit Date	Audit Reason
<p>Management Report: Received a report that an employee misused her travel card. Results: Identified almost \$800 in either disallowed or wasteful purchases. Employee was terminated prior to the completion of the review for an unrelated performance matter.</p>	Accounts Payable	Complete	24-013I	1/9/24		
<p>Internal Hotline: Received an anonymous concern of inappropriate hiring practices Results: The report was forwarded to HR for investigation. They did not find evidence of inappropriate hiring practices.</p>	Retention Services	Complete	24-014I	2/19/24		
<p>Internal Hotline: Received an anonymous complaint that of inconsistent practices related to offsite team building, and a lack of transparency of raises and bonuses. Results: The report was forwarded to Operations staff and HR. Offsite meetings require upper level approval, the intent of such meetings being aligned with departmental goals. It was also discovered that management were trained in the merit cycle and share information with their employees. No wrongdoing was identified.</p>	Retention Services	Complete	24-015I	2/19/24		

Description	Division/Campus	Status	Project No.	Report Date	Last Audit Date	Audit Reason
<p>Internal Hotline: Received 3 separate anonymous concerns related to student retention practices conflicting sometimes with enrollment goals, CARE team concerns and other accusations directed towards management of those areas. Results: The reports were referred to the managers in those areas. Management spoke with specific employees on the Waco campus to explain retention practices. They reviewed Maxient reports, and determined reports were acted on timely. And revised language to more clearly communicate to people making reports fo concerns that those concerns are being received and acted upon. There is no evidence that wrongdoing took place.</p>	Retention Services	Complete	24-012I, 20I & 21I	2/25/24		
<p>Internal Hotline Report: Received a concern through Ethical Advocate regarding assistance given to a Dual Enrollment student. Results: Determined no compliance steps were disregarded, and action that was taken was reviewed and approved by various levels of management.</p>	Dual Enrollment/Retention Services - Marshall Campus	Complete	24-027I	5/16/24		

Description	Division/Campus	Status	Project No.	Report Date	Last Audit Date	Audit Reason
Request by management: We were notified of questionable travel card transactions by an employee. Results: We identified isolated instances where charges for travel expenses were more than available alternatives. Management implemented procedures to correct this activity.	HR	Complete	24-0261	6/28/24		
Request by management: Expressed concerns about certain data on a tax related document. Results: An accounting firm is currently reviewing the results of the investigation, and helping formulate corrective actions.	Payroll	In progress				

Glossary	
HR	Human Resources
IA	Internal Audit
OIT	Office of Information Technology
SAO	State Auditor's Office
TEC	Texas Education Code
TAC	Texas Administrative Code
THECB	Texas Higher Education Coordinating Board

**Construction Audits
Status Report
June 27, 2024**

In Progress

TSTC - Project Name	Contractor	Estimated Substantial Completion	GMP	Agreed to Audit Issues	Audit Cost	Status from R. L. Townsend Construction Audit Services
JBC Remodel	Imperial	02/28/2024	\$ 13,020,898	\$ 47,812	\$ 16,500	Audit Entrance Meeting 4/26/2023 2/28/2024 - AQ Log sent with cost reviewed thru PA 13, 1/31/2024 With added changes, Imperial estimates the final Pay App to be in July. Awaiting the backup for the final payroll billed.
Marshall CCAP	Bartlett Cocke	11/01/2024	\$ 9,163,093	TBD	\$ 16,500	Audit Entrance Meeting 2/14/2024 Bartlett Cocke in process of uploading requested documentation. 3 pays have been reviewed. Nothing significant identified yet. Audit is in early stages.
Waco Annex	Mazanec	12/05/2024	\$ 12,000,000	TBD	\$ 16,500	Audit Entrance Meeting 8/17/2023 Initial Pay App Review - Pay Apps 1-4, 12/31/2023 Met with Mazanec and TSTC Construction Team to discuss backup GC Payroll Review in Process. Audit is progressing. Nothing significant identified yet.
Harlingen CCAP	JT Vaughn	04/22/2025	\$ 46,526,257	TBD	\$ 52,000	Entrance Meeting was held on 5/23/24. An agreed upon evolving process has been developed for GC labor reviews.
EEC & TSC Reno (CSP)	Imperial	04/29/2025	\$ 9,300,000	TBD	\$ 8,500	Entrance Meeting was held on 4/17/24. Audit is progressing.
Abilene CCAP	Imperial	06/16/2025	\$ 20,000,000	TBD	\$ 22,000	Audit Entrance Meeting 11/15/2023 Construction start pending NTP
Fort Bend CCAP	JT Vaughn	08/01/2025	\$ 42,000,000	TBD	\$ 48,000	Audit Entrance Meeting 2/22/2024 Initial audit document request received Initial Review in Process - Pay Application & GC Payroll Rates. An agreed upon evolving process has been developed for GC labor reviews.
Waco CCAP	Rogers O'Brien	09/02/2025	\$ 59,600,000	TBD	\$ 65,000	Audit Entrance Meeting 11/17/2023 GMP Review with Construction Team R-O updated they have started to mobilize R-O requested an April audit check-in meeting
Total			\$ 211,610,248	\$ 47,812	\$ 245,000	

Complete

TSTC - Project Name	Contractor	Substantial Completion	Final Contract Value	Audit Recovery	Audit Cost	Status from R. L. Townsend Construction Audit Services
Griffith Hall	Lee Lewis	completed	\$ 21,212,688	\$ 278,281	\$ 15,000	Final Report Issued 7/20/2022
FTB Welding	Bartlett Cocke	completed	\$ 8,089,004	\$ 55,977	\$ 11,000	Final Report Issued 8/24/2023
Total			\$ 29,301,692	\$ 334,258	\$ 26,000	
Grand Total			\$ 240,911,940	\$ 382,070	\$ 271,000	



**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
Procurement Card Program Audit (24-018A)	1.	While internal controls are well designed, some are not being consistently applied.	Vendor hold checks are not consistently performed; missing receipt; active cards did not reconcile to Workday; former employees cards not immediately cancelled; limits not always followed; food purchases did not always include the required additional documentation; \$3,500 in potential duplicate payments to a single vendor; 20 purchases on the Amazon account that did not follow the established protocol; published P-card guidelines were significantly different than current procedures.	1.1 Enhance financial controls by implementing monthly reconciliation of procurement cards, improving cardholder training, establishing a timely card cancellation process, and monitoring spending patterns. Additionally, Procurement Services is developing a policy related to business meals, official functions and entertainment-like expenditures directly related to or associated with the active conduct of official TSTC business. Procurement card guidelines have already been updated and communicated to current cardholders.	Jessica Chavira	10/31/24

CRIMES Software Audit (24-019A)	1.	We identified 13 of the 48 required TAC 202 controls managed by College personnel that either need to be implemented, or enhanced. Additionally, we were unable to test 15 of the 48 controls because the vendor failed to provide necessary information.	13 controls needed to be improved. 15 could not be tested because vendor failed to provided requested information.	1.1 We will facilitate a meeting between the vendor and OIT personnel to help get a full understanding of those TAC 202 controls that could not be tested during the audit. If the answers are unsatisfactory, we will pursue another solution in which security can be fully verified. We will also request OIT take over the administration of the software, comparable to other software utilized by the college.	Becerra	12/1/24
--	----	---	--	--	---------	---------

Internal Network Penetration Test (24-024A) - Marshall Campus	1.	There are opportunities to improve physical and IT security controls on campus.	4 employees were social engineered; identified 4 open ports on the internal network; identified 5 devices on the employee internal network using default administrator credentials; found one building unlocked after business hours; we entered a building during business hours when no employee was present with car keys accessible.	1.1 Contact each employee who was engineered, and require additional training; lock unoccupied buildings.	Day	Immediately
				2.1 Disable all ports and change all administrative passwords.	McKee	Immediately

Quality Assurance Review of Internal Audit - performed by Baylor Audit Staff	1.	Internal Audit received a rating of "Generally Conforms."				
---	----	---	--	--	--	--

Student Grievances Audit (24-022A)	1.	No findings noted.				
---	----	--------------------	--	--	--	--

TAC 202 Compliance – Quarterly Update (24-009A)	1.	No more controls were implemented. There are 7 controls still outstanding, but they are not ready to be tested.
--	----	---

FY 2023 Single Audit Evaluation Management Letter by the Texas Higher Education Coordinating Board	1.	No findings noted.
---	----	--------------------



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

Completion Summary			
	3/31/24	3/31/24	Audits cleared from (Added to) Schedule
Audits from FY 2023	5	4	1
Audits from FY 2024	3	6	(3)
Net Total	8	10	(2)

Highlights:

Procurement Card Fraud Investigation (23-0161): Complete
Personal Property Audit (23-003A): RFID implementation is over 60% 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
---------------------------------	------------------------	---------------------	-----------------------------------	-------------------------------	-----------------------

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
T Drive Audit (23-012A), McKee	1. We identified 4 of 41 required TAC 202 controls that still need to be implemented. These controls relate to audit logs and periodic testing of the back-up files. The control related to testing back-ups was implemented during our audit, but we would like more history of operation before concluding it is fully implemented.	1.1 OIT will implement a SIEM solution that will be managed and monitored by a 3rd party. This will provide TSTC with a logging solution that will alert for logging failures, provide alerting upon suspicious activity and will maintain the logs for the specified retention period.	Ongoing: Testing will be part of the quarterly TAC 202 follow-up.	A SOC and SIEM solution is still being discussed and researched. There are prerequisites to this topic, including a central logging capability and possibly a central monitoring tool. The timing of this item will change based on this. We still expect to implement phase one of this solution in FY2024.	8/31/24
		1.2 OIT will have a written plan to periodically test system backup and recovery that will include the creation of an OIT ticket to track the testing of the T:Drive. This plan will include a spreadsheet where the tickets will be tracked for the annual backup and recovery testing of the T:Drive.	Ongoing: Progress is being made, but not yet completed.	This testing will be moved into our Disaster Recovery plan and Testing, which is under the IT General controls section of this document.	5/15/24

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
Personal Property Verification Audit (23-003A), Boykin	1.	There are opportunities to improve control processes to ensure accurate recordation and safeguarding of personal property more effectively and efficiently.	1.1 RFID asset tag technology will be implemented as part of the annual inventory process. The RFID initiative will be implemented in phases, strategically beginning with specific high value and/or high-volume areas.	Ongoing: On 3/12/24, we met with accounting personnel and the newly hired Statewide Director of Property Management who oversees the property accountability process. We discussed all known issues and necessary improvements. An RFID system has been acquired, and implementation is in progress. We will closely monitor progress over the next several months. Implementation of CAP 1.1 and CAP 1.3 should significantly strengthen the system of controls. RFID implementation is 60% complete as of 6/14/24. Expected completion is still 8/31/24.	We now have confirmed onsite days with the vendor. We are hosting two training events, first will be in Waco on 4/23 and the second will be in Harlingen on 5/1. We will be bringing in inventory control from all of the other campuses in for this training. Once complete, they will start to work on their respective campuses.	Anticipated date of completion is 8/31/2024
			1.2 "Spot checks", each month, will be performed by Inventory Control staff beginning no later than September 2023. The spot checks will focus on high volume / high risk groups of assets. We will target no less than 50 assets each month, hopefully increasing spot check volume as the new process matures.	Ongoing:- See note in 1.1		Anticipated date of completion is 8/31/2024

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 IT General Controls (23-018A), McKee	1.	We identified 6 of 34 required TAC 202 controls that still need to be implemented. These controls relate to testing of the contingency and disaster recovery plans, physical and environmental access controls to the data centers, and the need to consider enhancements to controls related to mobile devices.	1.1 Implement a solution to assist in the authorizing, monitoring, and control of mobile devices accessing TSTC information pending available funding to implement the solution. This solution will allow TSTC to be able to monitor mobile devices that are enrolled in a Bring Your Own Device (BYOD) plan.	Ongoing		8/31/24
			1.2 Update and test the disaster recovery plan by performing a tabletop exercise which will serve as training for those involved in the Disaster Recovery Plan. This plan will be updated and tested on an annual basis going forward.	Ongoing: Progress is being made, but not yet completed.	Currently reviewing DR Plan and Recovery Procedures. The testing dates could change depending on how long it take to update the documentation.	1/31/24
Payroll and Benefits Proportionality Audit (23-019A), Sill, Motwani	1.	Select payroll deductions for some employees are not being calculated properly by Workday. Additionally, Workday is not correctly handling TRS benefits for new members past their 90th day of employment.	1.2 We have engaged our Workday vendor to assist with the correction. The calculation will be correct by October 2023, and Payroll will continue to audit all new hires for correct calculation until the correction is tested and verified.	Ongoing: 6/20/24 This issue has not been resolved. Due to the low population, this is affecting, other more important issues have taken priority. A completion date has been set.		12/31/24

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
	2.	Workday is including non-benefits eligible pay items in the proportionality calculation.	2.1 The Accounting Office will work with Workday consultants to find the best solution for this. In the meantime, the Accounting Office will continue to review and spot check the proportionality in the monthly payroll review.	Ongoing: 6/20/24 This issue has not been resolved. Due to the low population, this is affecting, other more important issues have taken priority. A completion date has been set.		12/31/24
Public Funds Investment Act Audit (24-005A), Motwani	1.	We identified three minor exceptions related to incorrect maturity dates and an interest rate reported on the May 31, 2023, Quarterly Investments Report. Additionally, we noted one exception on the May 31, 2023 Pledged Collateral Report, which overstated collateral by \$11,192. With stated collateral adjusted for the error, the collateral amount was still more than sufficient.	1.1 The investment report and collateral report will be reviewed more closely, and an automated element will be added to prevent human error. By February 29, 2024, Workday reports will be created to pull this data directly from bank statements rather than manually inputting this data.	Ongoing 6/20/24 The automated Workday report has not yet been created.		12/31/24
PCI Audit (24-002A), McKee, Franke	1.	Twenty four of the 103 applicable controls we tested require attention. Primarily, those controls required better documentation. But, we did identify opportunities to improve anti-virus software implementation, multi-factor authentication, and the incident response plan.	1.1 Documentation and processes will be created to address the findings.	Ongoing		12/31/24

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
Safety & Security Audit (24-007A), Various Managers	1.	There are safety processes and issues throughout the College that need to be improved.	1.1 All corrective actions will be implemented no later than August 31, 2024. Those will include improvements in monitoring of various processes, improved documentation and frequency of self-inspections, updated evacuation routes, more frequent performance of fire drills, and other necessary improvements to address the specific observations listed above.	Ongoing		8/31/24
Procurement Card Program Audit (24-018A), Chavira	1.	While internal controls are well designed, some are not being consistently applied.	1.1 Enhance financial controls by implementing monthly reconciliation of procurement cards, improving cardholder training, establishing a timely card cancellation process, and monitoring spending patterns. Additionally, Procurement Services is developing a policy related to business meals, official functions and entertainment-like expenditures directly related to or associated with the active conduct of official TSTC business. Procurement card guidelines have already been updated and communicated to current cardholders.	Ongoing		10/31/24

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
CRIMES Software Audit (24-019A), Becerra	1.	We identified 13 of the 48 required TAC 202 controls managed by College personnel that either need to be implemented, or enhanced. Additionally, we were unable to test 15 of the 48 controls because the vendor failed to provide necessary information.	1.1 We will facilitate a meeting between the vendor and OIT personnel to help get a full understanding of those TAC 202 controls that could not be tested during the audit. If the answers are unsatisfactory, we will pursue another solution in which security can be fully verified. We will also request OIT take over the administration of the software, comparable to other software utilized by the college.	Ongoing		12/1/24
Internal Network Penetration Test (24-024A) - Marshall Campus, Day, Mckee	1.	There are opportunities to improve physical and IT security controls on campus.	1.1 Contact each employee who was engineered, and require additional training; lock unoccupied buildings.	Complete		Immediately
			2.1 Disable all ports and change all administrative passwords.	Complete		Immediately
Travel Card Investigation (24-026I) - Mayfield, Vogelsinger	1.	We identified isolated instances for an employee where charges for travel expenses were more than available alternatives.	1.1 Employee will reimburse a shuttle service; ocast-effective options will be adhered to; all flights will be booked through Concur; all T-card purchases will be supported by receipts.	Ongoing		12/31/24



Internal Audit Department

Audit Report

Procurement Card Program Audit (24-018A)

May 14, 2024

**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 have recently completed an audit of the Procurement Card (P-card) Program. The primary objectives of this audit were to ensure that purchases made on P-cards were within allowed rules, and only for legitimate College purposes. We also verified select internal controls which help achieve these objectives. The scope of the audit included all purchases made by P-cards in calendar year 2023.

To accomplish our objectives, we reviewed approximately 5% of all P-card purchases in 2023. 295 purchases valued at over \$550 thousand were scrutinized to ensure they followed applicable purchasing rules, and were legitimate. We reviewed cardholder agreements and training to ensure cardholders were aware of their responsibilities. We verified active P-cards reconciled to those recorded in Workday to ensure purchases made on P-cards were automatically recorded. Transaction and billing cycle limits were tested, as was the timely closing of P-cards when employment was terminated. Payments made to Citibank were tested for timeliness and correctness. Finally, we identified select trends that we noted during a review of purchasing data that helped us focus on risks. Purchases from Amazon using the College's Amazon account were also similarly scrutinized. Because this is a separate process from the P-card process, we performed separate tests on just these purchases.

We did not identify any obviously inappropriate or fraudulent purchases made on P-cards or from Amazon. Purchases generally complied with fiscal limits, and the types of items that are allowed to be purchased. There were generally documented exceptions for purchases that were outside of stated guidelines. Employees who hold P-cards received specific training to ensure they were aware of expectations and requirements. Payments to Citibank were timely and correct. The College's Amazon account was restricted.

We did identify a need to improve the operation of several key controls over P-card use, however. Details of that observation are stated in Finding #1.

Introduction

P-cards are business credit cards issued by Citibank. The College maintains a P-card program to help facilitate an easy method of purchasing lower cost, generally commodity type of items and/ or services, or routine types of purchases.

Currently, there are 537 active procurement cards. Employees who are assigned P-cards can purchase items such as books, lab supplies, office supplies, safety supplies, tools and hardware, conference registrations, and courses and seminars. P-cards are segregated into 3 categories: those with a single transaction limit of \$10,000 (reserved for managers), those with a single transaction limit of \$15,000 (reserved for specialized operations such as cafeterias, bookstores, and facilities) and those with a single transaction limit of \$5,000. The majority of cards fall within the latter category.

Between January 1, 2023, and December 31, 2023, there were 32,587 p-card transactions, totaling \$11,143,438. The 3 highest spending categories were utilities, equipment and material, and purchases at specialized stores. The exact items are difficult to categorize because they are only available on detailed receipts that are uploaded as an image after purchases are made. From our testing, we noted that most purchases were related to supplies, utilities, and maintenance or equipment or facilities.

Each use of a P-card is automatically recorded in Workday due to an interface between that system and Citibank. P-card users must upload a detailed receipt for each purchase that clearly documents each purchased item. Budget account managers approve each P-card transaction in Workday. There are several opportunities by individual managers and the Travel and Card Services Department to prevent and detect P-card misuse.

The P-card program is overseen by the Travel and Card Services Department, under the direction of the Executive Director of Purchasing. Employees within Travel and Card Services review all P-purchases for compliance. This same group issues new cards, provides training to new P-card holders, and cancels cards when employees terminate or no longer need a card. They also oversee the use of the College's Amazon account.

Objectives

The objectives of the audit were to determine whether:

1. P-card purchases follow purchasing rules, and are legitimate.
2. Reasonable internal controls have been designed and implemented to ensure purchases made using P-card follow established guidelines.

Scope & Methodology

The scope of our audit included all P-card purchases made between January 1, 2023, and December 31, 2023. We utilized P-card guidelines available on the Procurement section of the Portal, SOS FA 1.16 Purchasing Authority, and the actual flow of the processes as documented by us in a flowchart after discussions with personnel. Some of the testing involved tracing purchases to supporting documentation, reviewing training records, considering purchases in light of the employee's official duties, reconciling existing cards per Citibank records to Workday, and reviewing payments.

General Observations

Staff within Travel and Card Services Department were responsive to all requests during this audit, and requested a thorough review so that they can enhance their current processes. Workday has simplified the processing and recordkeeping of P-card purchases by making it more timely, accurate, and secure. Detailed receipts are uploaded to Workday that document the exact purchases, and employees are buying items that support their

responsibilities and functions. When items are shipped from a vendor, they are being shipped to College locations.

Summary of Finding

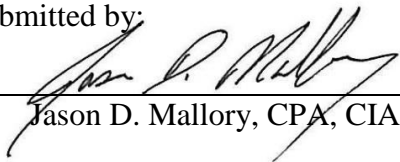
While internal controls are well designed, some are not being consistently applied.

Opinion

Based on the audit work performed, purchases made on P-cards generally follow purchasing rules, and are legitimate. But internal controls that support these objectives require attention to ensure they are being consistently followed. Finding #1 supports this observation.

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

May 14, 2024

Date

AUDIT FINDING DETAIL

Finding #1: While internal controls are well designed, some are not being consistently applied.

Criterion: We reconciled active all P-cards per Citibank to recorded cards per Workday. We tested 295 P-card purchases to verify they complied with purchasing rules, and were legitimate. We also tested a sample of purchases made on the College Amazon account. We noted the following issues that are control related:

- Vendor hold checks are not consistently being performed and/or documented on purchases over \$500.
- Several purchases were not supported by an itemized receipt.
- We found differences in the number of active cards to those recorded in Workday.
- We identified 15 former employees whose cards were not immediately cancelled after their last day of employment. It took an average of 24 days to cancel the cards in the group we identified. One person's card was active 146 days after his employment ended.
- Limits for single purchases and/or total purchases during a single billing cycle were not always followed or the approvals for the exceptions were not always documented.
- Several food purchases did not include the required additional supporting documentation of who, what, where, when and why. Food related purchases account for over 5% of all purchases made on P-cards.
- We identified approximately \$3,500 in potential duplicate payments to a single vendor.
- We found 20 purchases on the Amazon account that did not follow the established protocol. These were made shortly after the process changed.
- The published P-card guidelines were last updated in 2017. Current processes are significantly different than they were in 2017.

Consequences: Increased probability for purchases to either not be appropriate and or legitimate.

Possible Solutions: Perform a more thorough review of the transactions by the Travel and Card Services Department, with exceptions appropriately resolved and escalated, as appropriate; reconcile active cards to those listed in Workday, with exceptions being fixed; incorporate a step in the campus clearing process to deactivate P-cards held by people who will no longer be employed; implement a process to identify duplicate payments; update P-card guidelines to reflect current processes.

Management Response

Management of Procurement Services agrees with the observations made in the audit. By October 31, 2024, Procurement Services will enhance financial controls by implementing monthly reconciliation of procurement cards, improving cardholder training, establishing a timely card cancellation process, and monitoring spending patterns. Additionally, Procurement Services is developing a policy related to business meals, official functions and entertainment-

like expenditures directly related to or associated with the active conduct of official TSTC business. Procurement card guidelines have already been updated and communicated to current cardholders. Jessica Chavira, Director of Payment Services, will be responsible for the implementation of this corrective action plan.



Internal Audit Department

Audit Report

CRIMES Software Audit (24-019A) Campus Police

May 23, 2024

**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 performed an audit of the Criminal Research Information Management and Evaluation System (CRIMES) utilized by the TSTC Police Department (Police). CRIMES is software developed by a public university in Texas to aid in the recordation requirements of the daily operations of law enforcement departments across the State of Texas. CRIMES allow the Police to store and access detailed crime related information. The purpose of this audit was to verify compliance to 48 related TAC 202 controls.

We tested or attempted to test system access, training, audit logs, system identification and authentication, password management, and other integrity related controls. We also included controls related to periodic maintenance, and baseline and system configurations.

We were able to test 33 of the 48 controls that were within the scope of this audit. Of those, 13 require improvement. We were unable to test the remaining 15 controls because the software developer failed to provide information we repeatedly requested. This included procedures related to periodic software updates, access to College data, and system configuration. The following table summarizes the required TAC 202 controls we tested or attempted to test, and our results:

Control Family	Implemented	Implemented with Recs	Not Implemented	Could Not Verify
Access Controls	6	0	4	0
Awareness and Training Controls	4	0	0	0
Audit and Accountability Controls	2	0	2	5
Configuration Management Controls	0	0	0	4
Contingency Planning Controls	0	1	4	0
Identification and Authentication Controls	5	0	0	0
Maintenance Controls	0	0	0	2
Personnel Security Controls	2	0	1	0

Risk Assessment Controls	0	0	1	0
System and Service Acquisition Controls	0	0	1	0
System and Communication Protection Controls	0	0	0	2
System and Information Integrity Controls	0	0	0	2
Total	19	1	13	15

Introduction

CRIMES is records management software used by the Police on the Waco, Harlingen, and West Texas campuses. The software processes and stores sensitive information on all types of interactions that police officers have daily, to include all forms of crime. Sensitive criminal and victim information is gathered and stored on a virtual database server located on the Waco campus, accessible by both the software developer and personnel in the Office of Information Technology (OIT). Originally acquired in 2011 at an annual cost of \$15,000, the current annual cost is \$21,000 for a license fee, system maintenance, training, and related services. It renews in October of each year.

The Police have acted as administrators for CRIMES since it was purchased. OIT’s involvement has, to date, been limited to managing the server the data is stored on.

Objectives

The objectives of the audit were to verify controls in place to ensure security, integrity, and availability for the CRIMES using TAC 202 control requirements.

Scope & Methodology

The scope of our audit included all processes and procedures currently in place at the time of this audit as they relate to the CRIMES. The Security Control Standards Catalog, Version 2.1 promulgated by TAC 202 formed the basis of our testing. To achieve our objectives, we interviewed key personnel in the Police Department and OIT, reviewed system logs/configurations, tested access, and verified controls related to encryption, back-up and recovery, and training. We did have a scope limitation in this audit due to the vendor failing to provide information we repeatedly requested. Accordingly, we cannot offer an opinion on 15 of the 48 controls that were within the scope of this audit.

General Observations

Controls related to password management, identification, and authentication are strong. Passwords are masked when entered, and accounts are locked after a set number of failed login attempts. Multi-factor identification is also in place. Remote access is controlled by the colleges virtual private network services. Training is in place before users are granted access. Audit logs we were able to review were time stamped and contained sufficient information to recreate activity, should it be needed. Furthermore, the software provides the Police a tool to accurately college necessary crime-related data.

Summary of Finding

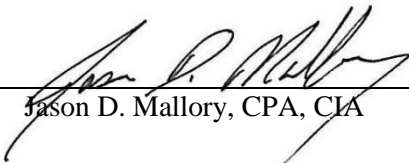
We identified 13 of the 48 required TAC 202 controls managed by College personnel that either need to be implemented or enhanced. Additionally, we were unable to test 15 of the 48 controls because the vendor failed to provide necessary information.

Opinion

Based on the audit work performed, governance over CRIMES needs to be improved. This may include seeking another software which meets both the Police's needs and the need for security of the data.

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

May 23, 2024
Date

AUDIT FINDING DETAIL

Finding #1: We identified 13 of the 48 required TAC 202 controls managed by College personnel that either need to be implemented or enhanced. Additionally, we were unable to test 15 of the 48 controls because the vendor failed to provide necessary information.

Criterion: The TAC 202 Security Controls Standard Catalog specifies the minimum information security controls to implement for all State information and information systems. For each required control, Internal Audit inquired and reviewed policies and procedures, users' access roles and privileges, security settings, etc.

We determined that 13 of the 48 controls were not implemented.

Control Family	Not Implemented
Access Controls	4
Audit and Accountability Controls	2
Contingency Planning Controls	4
Personnel Security Controls	1
Risk Assessment Controls	1
System and Service Acquisition Controls	1
Total	13

We were unable to test 15 of the 48 controls, therefore, cannot offer an opinion on their state of implementation:

Control Family	Could Not Verify
Audit and Accountability Controls	5
Configuration Management Controls	4
Maintenance Controls	2
System and Communication Protection Controls	2
System and Information Integrity Controls	2
Total	15

Consequences: Increased risk of exposure and loss to sensitive crime related information handled by the TSTC Police.

Possible Solutions: We recommend OIT takeover the administration of the software, comparable to other software utilized by the College. We also recommend that all required TAC 202 controls be verified as implemented. If the vendor fails to provide information that allows for assurance that controls are in place, we recommend another software be implemented after a thorough risk assessment is performed.

Management Response

Management of the Police Department agrees with the observations made in the audit. 15 of the 48 TAC 202 security controls were unable to be tested because the vendor failed to provide necessary information after several requests were made by the auditors. When the software was originally implemented in 2011, a decision was made by previous managers within the Police Department and OIT that the administration of the software would be handled within the Police Department. By not including OIT, a complete understanding of TAC 202 requirements, and communication with the vendor of the importance of being able to validate the required controls, were not achieved. By 12/1/24 we will facilitate a meeting between the vendor and OIT personnel to help get a full understanding of those TAC 202 controls that could not be tested during the audit. If the answers are unsatisfactory, we will pursue another solution in which security can be fully verified. We will also request OIT take over the administration of the software, comparable to other software utilized by the college. Police Lieutenant Eduardo Becerra will be responsible for implementation of this corrective action plan.



Internal Audit Department

Audit Report

**Internal Network Penetration Test (24-024A)
Marshall Campus**

June 6, 2024

**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 April 8, 2024, and May 10, 2024, we performed vulnerability scans and penetration testing on the Marshall Campus. This test was primarily directed at identifying internal network vulnerabilities, however, we also tested the physical security of buildings.

The primary objective of this project was to ensure the physical and logical security of information technology assets directly supporting the confidentiality, integrity, and accessibility of College information. This test attempted to detect vulnerabilities to help prevent attacks from unauthorized or inappropriate activity on the Marshall Campus. We tested various security controls and procedures, to include the segregation of College and guest networks. Our tests included scanning networks to identify open ports that should be restricted, identifying default user credentials being used on network devices, social engineering a sample of employees to identify cybersecurity awareness, and attempting to gain unauthorized access to buildings and rooms where sensitive information may be stored. We also attempted to access employee computers when they were not present, and pulled on doors after business hours. We conducted a similar test on this campus in fiscal year 2021.

We determined that campus employees generally secure access to sensitive information by locking their offices and/or computers when not in use, and by not disposing of sensitive documents in publicly accessible trash cans. We found employee and guest wireless networks are segregated, and protected by secure logon protocols and encryption. Access to those networks is also restricted to the inside of buildings. IT-related closets and rooms are restricted by locks that require both a physical key and badge swipe, and are monitored by video surveillance. Employees are trained on cybersecurity risks. Finally, buildings are locked after business hours.

We were able to social engineer 4 employees through phishing emails which could have compromised their Workday credentials. Even though multi-factor authentication is in place which would have probably prevented any actual unauthorized access, these employees were notified anyway because their actions heightened security risks. We also identified 4 active ports on the internal employee network that were open, and we found 5 devices on the internal employee network using default administrator login credentials. We viewed these as opportunities to exploit in hacking and intrusion attacks by bad actors. Finally, we identified 2 opportunities to better restrict physical access that would improve general security.

Introduction

The Office of Information Technology (OIT) Division assists the College with its IT needs by maintaining secure networks, providing end-user support and training, assisting with IT purchases, maintaining critical databases, and offering critical application support. OIT has 1 Field Support Technician dedicated to the Marshall Campus. IT security personnel located on other campuses provide remote support to the campus.

All campus employees have a role in ensuring assets and data are protected. They are expected to lock doors and computers when not in use, be aware of cybersecurity attacks through periodic training, and maintain a general awareness of suspicious activity and risks. The Marshall Campus is managed by a Provost, with instructional and other support functions located on campus.

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 appropriate security controls in place to detect and prevent attacks.
- ensure unauthorized individuals on campus are reasonably prevented from accessing privileged systems or sensitive data.
- assess internal employee guest networks are segregated.
- identify the usage of default logon credentials on network devices.
- verify training on cybersecurity risks are being completed periodically, and applied.
- identify real-world attack vectors that are present.

This test was not intended to verify all risks the campus and IT may face during an attack.

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 campus employee behavior, especially their awareness of, and vigilance against, potential 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 800-128 – Guide for Security Focused Configuration Management of Information Systems.
- NIST 800-53r5 - 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 login credentials to 36 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

We found the campus to be well secured. Buildings were locked after hours, and employees secured their computers and offices when they were away from them. Most of our phishing attempts failed, and our attempts were immediately reported to OIT as suspicious. In fact, we had

to ask OIT to allow the emails to go through because they were recognized and restricted so quickly. We also did not have anyone who responded to our phishing attempts that also responded in our test in 2021, indicating training and awareness have improved.

Computers available to students in open areas are restricted from the internal network and are managed with administrator accounts. And finally, there is an increased number of personnel who have attended the optional Cybersecurity and You training offered by the Office of Information Technology. Campus management has done a commendable job in increasing and fostering general and cyber security awareness.

Summary of Finding

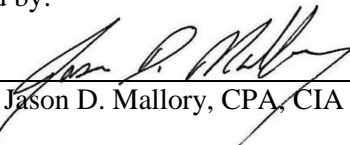
There are opportunities to improve physical and IT security controls on campus.

Opinion

Based on the audit work performed, IT assets and information are generally well protected on the Marshall Campus. Some controls and behaviors need to be improved, though.

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

June 6, 2024

Date

AUDIT FINDING DETAIL

Finding #1: There are opportunities to improve physical and IT security controls on campus.

Criterion: We made telephone calls and sent emails to 36 employees on the Marshall Campus in an attempt to social engineer their logon credentials to the College’s main database. We reviewed the training records of these same employees to ensure they completed required cyber security training. We searched for vulnerabilities and devices with default administrator credentials by scanning open ports. Finally, we attempted to access campus buildings and rooms after business hours or at times when employees were not present. We identified the controls or behaviors following that need improvement:

- Four employees responded to our social engineering email by presumably providing their logon credentials to Workday. One of these employees did notify OIT of our attempt which resulted in the test being temporarily shut down.
- We identified 4 open ports on the internal network that we could have attempted to exploit to gain unauthorized access to network.
- We identified 5 devices on the employee internal network using default administrator credentials. Again, we could have attempted to exploit these devices to gain unauthorized access to data, or simply been disruptive.
- We found one building unlocked after business hours. The building did not contain any high value equipment or sensitive records. And, we entered a building during business hours when no employee was present. Keys to vehicles were readily accessible.

Consequences: Increased risk of inappropriate access to sensitive data or assets.

Possible Solutions: We recommend the employees be reminded of their responsibilities to protect access to systems, and the methods used by bad actors to gain such access. We also recommend all buildings be locked after business hours, and keys to vehicles secured properly. Finally, we recommend all open ports be secured, and all default logon credentials to devices on the network be changed.

Management Response

Management on the Marshall Campus agrees with the observations made in the audit. The following corrective/preventative actions have either been put in place or are in progress. Four employees who report to other managers provided information to a social engineering email that she should have disregarded. Bart Day, Provost, has contacted each employee to inform them of the test results and each will be required to take cybersecurity training taught by Scott Hodkinson in IT Risk Management on June 10, 2024. In addition, this training has been offered up as a refresher to all campus employees in an effort to reduce the chance of recurrence. The Physical Plant building was found to be unoccupied and unsecure during business hours. From this point forward, the building will be locked when personnel are not present. A building, the “gym” was found to be unsecured after business hours. Campus Security has been asked to redouble their

efforts to check all facility doors at the close of the business day. Campus Provost Bart Day will be responsible for implementation of these corrective actions.

Management of the Office of Information Technology agrees with the observations made in the audit. The following corrective actions have been completed:

- Open Ports: OIT disabled all open ports found during the Pen Test on the switches. This was remediated in ticket number 25576161.
- Printers with no administration passwords: All printers that were found to not have administrative passwords changed have been remediated. This was remediated in ticket number 25576126.

Larry McKee, Sr. Director of IT Security and Compliance, ensured these corrective actions were immediately implemented.



Baylor University

June 14, 2024

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

Dear Mr. Mallory,

We have completed an external quality assurance review on the Internal Audit Department of the Texas State Technical College (TSTC). In conducting our review, we followed the standards and guidelines contained in the Peer Review Manual published by the State Agency Internal Audit Forum.

The primary objective of the review was to provide an opinion on whether the internal auditing program 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, we collectively refer to these as "the Standards".

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.

Results and Opinion

Based on the information received and evaluated during this external quality assurance review, it is our opinion that the TSTC Internal Audit Department receives a rating of *Generally Conforms*.

Key Strengths

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. Additionally, interviews with senior leaders and members of the board revealed a high degree of confidence in the audit function, with many complimenting the professionalism, thoroughness, and transparency of the audit team.

We would like to thank the TSTC Internal Audit staff as well as other TSTC representatives for their assistance during the review.

Sincerely,



Amanda R. Wallace, CPA
Chief Audit Officer
Baylor University



Internal Audit Department

Audit Report

Self-Assessment of Quality of Internal Audit (24-004A)
TEXAS STATE TECHNICAL COLLEGE
Internal Audit

September 22, 2023

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 completed a self-assessment of our processes and practices to ensure internal audit quality during the period of September 1, 2020, through August 31, 2023. The primary purpose of our review was to offer an opinion on whether Internal Audit achieved the basic requirements expected of internal audit activities at all institutions of higher education supported by the State of Texas. Those requirements are set forth by the Texas Internal Auditing Act (Tex. Gov't Code Chapter 2102), the Institute of Internal Auditors' (IIA) *International Standards for the Professional Practice of Internal Auditing and Code of Ethics*, and the U.S. Government Accountability Office's (GAO) *Generally Accepted Government Auditing Standards*. For purposes of this review, we collectively refer to these as the *Standards*.

The review was conducted in accordance to the State Agency Internal Audit Forum Peer Review Guidelines using the Compliance Standards assessment. The assessment focuses on numerous procedures we have implemented to ensure standards are met related to ethical behavior, independence, due professional care, and quality. It also addresses management practices within IA, the nature of work performed, and various performance and reporting standards. We reviewed the Internal Audit Charter, IA policies and procedures, and annual confirmations to the Audit Committee regarding IA's independence, review of the adequacy of the Internal Audit Charter and on our quality control program.

We feel IA generally conformed to requirements set forth by the Texas Internal Auditing Act (Tex. Gov't Code Chapter 2102), the IIA's *International Standards for the Professional Practice of Internal Auditing and Code of Ethics*, and the GAO's *Generally Accepted Government Auditing Standards* for the period we reviewed.

Introduction

Our self-assessment is required by both the Texas Internal Auditing Act and the IIA's *Standard 1311-Internal Assessments*. Our self-assessment documentation and conclusion on compliance will be validated by an external peer reviewer to ensure our self-assessment is appropriate, and to assist IA with maintaining the quality that is required.

Objectives

The purpose of this self-assessment was to verify Internal Audit at TSTC generally conformed to the Texas Internal Auditing Act (Tex. Gov't Code Chapter 2102), the IIA's *International Standards for the Professional Practice of Internal Auditing and Code of Ethics*, and the GAO's *Generally Accepted Government Auditing Standards* for the period under review.

Scope & Methodology

The scope of the review included all internal audit processes in place at TSTC from the period of September 1, 2020, through August 31, 2023. We utilized the Peer Review Manual developed by the State Agency Internal Audit Forum dated May 2017 (this is the most recent template) to form the basis of our self-assessment. That manual incorporates requirements from the Texas Internal Auditing Act, the IIA's *International Standards for the Professional Practice of Internal Auditing* and *Code of Ethics*, and the GAO's *Generally Accepted Government Auditing Standards*.

General Observations

IA has established policies and procedures and an Audit Charter that are reviewed annually as part of the quality control process. The Charter is also presented to the Audit Committee annually for their review, with documentation of the review being maintained. IA staff also sign a form annually, acknowledging receiving the IA policies and procedures manual and acknowledging the Procedures on Independence; confirmation of the department's independence is also sent to the Audit Committee annually. Confirmation of IA's program of quality control is also provided to the Audit Committee annually. IA reports administratively to the Chancellor and functionally to the Board of Regents, as required by the *Standards*, and meets with both at least on a quarterly basis, with audit correspondence or ad-hoc discussions taking place more frequently. IA has a formalized audit plan and risk assessment process, in which input is obtained from both IA, management, the Leadership Team, and the Board of Regents. In addition, IA has a formal internal quality assessment process which requires 40 hours of continuing professional education annually, having a standardized workpaper review process, and conducting post-audit surveys.

Summary of Findings

No findings noted.

Opinion

Based on the audit work performed, IA generally conformed to requirements are set forth by the Texas Internal Auditing Act (Tex. Gov't Code Chapter 2102), the IIA's *International Standards for the Professional Practice of Internal Auditing* and *Code of Ethics*, and the GAO's *Generally Accepted Government Auditing Standards* for the period we reviewed.

Submitted by:



Tahlia Pena

9/22/23

Date



Internal Audit Department

Audit Report

Student Grievances Audit (24-022A)

June 27, 2024

**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 Student Grievances process. The primary objective of this audit was to ensure a well-defined, effective process is in place to resolve student grievances in a timely manner without bias towards the students or employees. The scope of the audit included all grievances submitted from September 2022 through February 2024. Academic, non-academic directed at faculty, and grievances directed at general College processes were reviewed. SOS ES 3.24, Student Grievances and Complaints, (SOS ES 3.24) served the guidance for our testing, along with various regulations outlined in the SACSCOC Policy Statement and Texas Administrative Code (TAC) 1.116.

To accomplish our objectives, we reviewed 40 grievances. Grievances from every campus were included in our sample. For each grievance, we verified proper documentation was on file, communication and submission deadlines were met, and resolutions were reasonable given the circumstances and nature of each grievance. We also verified the clarity and ease of the process, and whether it is clearly communicated to students. We reviewed training records for individuals resolving the cases, the time to resolve each one, and whether associated records were safe and secure. Finally, we analyzed grievances for any trends, and inquired about whether similar work is performed to help identify and improve customer service issues.

Our testing revealed grievances were resolved timely and without apparent bias. We found the resolution to be reasonable based on the facts presented in each. The process is relatively easy to follow, closely mirrors policy and regulatory requirements, and is communicated and made available to students in several ways. We did identify some opportunities to improve training, documentation, and access to records. These were communicated to management in a separate letter because they are minor in nature or were not pervasive issues.

Introduction

SOS ES 3.24 defines a grievance as a disagreement or dissatisfaction where a student believes there has been an infraction, misinterpretation or improper action in violation of the College's rules, regulations or policies. Grievances can be academic, non-academic, or a complaint with the quality of customer service provided by an employee of the College, otherwise known as a Compact with Texans complaint. Between September 1, 2022 and February 29, 2024, the college received only 77 academic, non-academic and Compact with Texans grievances/complaints. Broken down by campus, those were comprised of 20 in Waco, 15 in Harlingen, 14 in Fort Bend, 10 in Sweetwater, 7 in Marshall, 2 in Hutto, 1 in Abilene, and 8 from online students.

Grievances are received by the Student Rights & Responsibility Department (SR&R), overseen by the Director of Case Management, who then forwards the grievance to an Associate Provost or Supervisor to provide a resolution to the student. Appeals to resolutions are reviewed by a Statewide Review Board made up of volunteer staff and faculty. One of the 3 co-chairs assigned to a case will inquire about availability of the 26-member committee and select 2 additional committee members to serve on a particular case. All decisions by this group are final. SR&R

falls within the Operations Division. They also review cases related to student conduct, supplemental applications, academic integrity and Title IX. These were outside the scope of this audit.

Objectives

The objective of the audit was to verify compliance with SOS ES 3.24. Efficient, effectiveness, and timeliness of the grievance process were primary considerations.

Scope & Methodology

The scope of our audit included grievances submitted between September 2022 through February 2024. We tested a total of 40 grievances. We used SOS ES 3.24, the SACSCOC Policy Statement and TAC 1.116 for our testing. Our tests included reviewing each grievance for proper documentation, timeliness and appropriateness of resolutions. It also included reviewing training records, access to grievance to grievance related documentation, trends, and the ease with which the grievance process can be used. Finally, communication of the available process to students was considered.

General Observations

We specifically noted how well documented and timely each grievance was handled. Grievances were thoroughly researched and considered resulting in resolutions appearing reasonable, fair, and unbiased. Finally, we took note of the limited number of grievances filed in the time period reviewed in this audit.

Summary of Findings

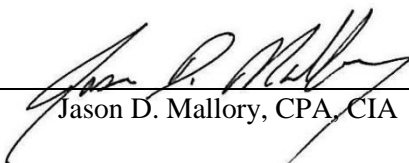
No material exceptions were identified.

Opinion

Based on the audit work performed, grievances are resolved fairly and efficiently, and in compliance with policy and regulatory requirements. The process is also well communicated, and records secured and well documented.

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

June 27, 2024
Date

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

August 2024

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, VC/CAE
 Subject: TAC 202 Compliance – Quarterly Update
 Date: July 1, 2024

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 April 1 through June 30, 2024, no more controls were implemented. There are currently only 7 controls from past audits to test. While action is being taken to implement/enhance the outstanding controls, they were not ready for testing when we inquired in late June. 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
As of December 2022	43	10	0	0	53

TWC Server

Original Audit: May 16, 2022

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
Jan 2023 – Mar 2023	47	4	0	0	51

T Drive

Original Audit: March 17, 2023

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
January 2024 – March 2024	37	0	4	0	41
November 2023 – December 2023	37	0	4	0	41
Difference	0	0	0	0	

IT General Controls

Original Audit: June 23, 2023

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted ^{Note 4}	Total
January 2024 – March 2024	24	6	3	1	34
November 2023 – December 2023	24	6	3	1	34
Difference	0	0	0	0	

Note 4: In Note 1 for the General Controls Audit conducted in FY 2017, management elected to not fully implement CM-11 related to end-user installed software. They feel compensating controls such as malware and the ability to restrict specific downloads from the internet assist with mitigating associated risks. They continue to accept this risk to the extent it is not fully controlled by completely restricting administrator rights on laptops and PCs. .

Submitted by:



 Jason D. Mallory, CPA, CIA

July 1, 2024

Date

cc: Mike Reeser, Chancellor/CEO
Dale Bundy, VC/CIO

June 17, 2024

Johnathan Hoekstra
Vice Chancellor & CFO
Texas State Technical College
3801 Campus Drive
Waco, TX 76705

RE: FY 2023 Single Audit Evaluation Management Letter
ALN: ARPA 21.027, GEER 84.425C, Perkins 84.048

Dear Johnathan 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 2023 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 Carson Beierman via email at carson.beierman@highered.texas.gov.

Sincerely,



Arby James Gonzales, CPA, CFE
Assistant Commissioner, Internal Audit and Compliance



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.