Board of Regents Meeting

Audit Committee Meeting

August 9, 2018
Waco, Texas

TEXAS STATE TECHNICAL COLLEGE

Board of Regents Meeting

Texas State Technical College
Connally Meeting & Conference Center
1651 E. Crest Drive
Waco, TX 76705

Thursday, August 9, 2018

10:30 a.m.

AGENDA

I. Meeting Called to Order by Audit Committee Chair Ivan Andarza

II. Committee Chair Comments

III. Minute Orders:

Proposed MO#

12-18(c) Revision of Proposed Audit Plan for Fiscal Year 2018 .....A-3

13-18(c) Proposed Audit Plan for Fiscal Year 2019 .....A-4

IV. Reports:

1. Status of Fiscal Year 2018 Audit Schedule & Other Projects A-14
   Jason Mallory

2. Summary of Audit Reports A-17
   Jason Mallory

3. Follow-up Scheduled & Status A-25
   Jason Mallory

4. PCI Compliance Audit.....A-37
   Jason Mallory

5. Marshall: Internal Network Penetration Test.....A-45
   Jason Mallory

Please note: Meetings are scheduled to follow each other consecutively and may start earlier or later than the posted time depending on the length of the discussions and the reports of preceding meetings. The estimated times are approximate and may be adjusted as required with no prior notice. Lunch will be at approximately noon.

6. Safety & Security Audit.....A-51
Jason Mallory

7. TAC 202 Follow-up Audit.....A-64
Jason Mallory

8. Fixed Asset Control Follow-up Audit A-66
Jason Mallory

9. Final Report – A Compliance Desk Review of Texas Educational Opportunity Grant A-69
Jason Mallory

10. Audit Delegation Request 719-FY18-001 .....A-72
Jason Mallory

11. Attestation Disclosures A-75
Jason Mallory

V. Adjourn

Please note: Meetings are scheduled to follow each other consecutively and may start earlier or later than the posted time depending on the length of the discussions and the reports of preceding meetings. The estimated times are approximate and may be adjusted as required with no prior notice. Lunch will be at approximately noon.

Board Meeting Date:	August 9, 2018	**Proposed Minute Order #:**	12-18(c)
Proposed By:	Jason D. Mallory, Director of Audits		
Subject:	**Revision of Fiscal Year 2018 Audit Plan**		

Background:

The Texas Internal Auditing Act, Chapter 2102 of the Texas Government Code, requires Board of Regents approval for the Annual Audit Plan (Plan) and any revisions. The Director of Audits recommends revising the Plan originally approved by Minute Order #25-17(c) on August 10, 2017, by removing two scheduled risk assessments, and replacing them with two audits within the Culinary Arts Programs on the Waco and Harlingen campuses.

Justification:

In April 2018, the Culinary Arts Program building on the Waco Campus was burglarized, and a vehicle was stolen. Campus police investigated that crime and identified the need to better secure the facility and improve controls for safeguarding assets, especially cash. Consequently, Executive Management requested an internal audit in that area to ensure appropriate controls are in place over all assets and resources. While not specifically requested, I want to perform an audit of the same program on the Harlingen campus because the same risks and controls are relevant. This would also afford the opportunity to determine whether controls and related processes are consistent across the campuses.

The original Plan included two risk assessments to be performed on the Ft. Bend campus in the Instructional Division. The primary purpose for those projects was to help educate newer instructors on various policies and procedures, and allow them to improve areas that are potentially deficient. I feel replacing the two risk assessments with two audits better addresses currently known risks. And because the requested projects are also within the Instructional Division, that same division benefits.

Additional Information: None

Fiscal Implications: Funds Available as Budgeted for Fiscal Year 2018.

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

Attachment(s): None

Recommended Minute Order: "The Board of Regents approves the revised audit plan for Fiscal Year 2018."

Recommended By:

Jason D. Mallory, Director of Audits

Board Meeting Date:	August 9, 2018 **Proposed Minute Order #:** 13-18(c)
Proposed By:	Jason D. Mallory, Director of Audits
Subject:	**Proposed Audit Plan for Fiscal Year 2019**
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 2019.
Attestation:	This Minute Order is in compliance with all applicable laws and regulations to the best of my knowledge.
Attachment(s):	Proposed Audit Plan – Fiscal Year 2019
Recommended Minute Order:	"The Board of Regents approves the audit plan for fiscal year 2019."
Recommended By:	Jason D. Mallory, Director of Audits

Audit Plan

Fiscal Year 2019

Proposed August 9, 2018

Executive Summary

The purpose of the Audit Plan (Plan) is to outline audits and other activities the Internal Audit Department will conduct during fiscal year 2019. The Plan was developed through collaboration with the Board of Regents (Board), Executive Management, and other managers throughout the College, as well as the Internal Audit staff. Risk assessment techniques, described later in this report, identified individual audits to be conducted during the year by considering the College's major activities and processes, which included its accounting systems and processes, administrative processes, and information technology systems. The Plan, its development, and approval are intended to satisfy requirements under the Internal Audit Charter (SOS GA.1.4) and the Texas Internal Auditing Act (TGC Chapter 2102).

The Plan relied upon risk assessments performed by departmental managers throughout the College of major activities and processes under their responsibility. Those assessments identified the impact specific risks rated by the Board and Executive Management would have on those major activities and processes. Seven high level risks were applied to 61 major activities and processes.

As result of those efforts, the Plan includes 15 full-scope audits, financial aid testing (A-133) by the State Auditor's Office (SAO), and a financial statement audit to be performed by an external accounting firm. Additionally, investigations will be performed on all complaints reported through the ethics hotline, assistance given to external auditors as requested, and follow-up audits performed on outstanding findings from previous audits. Known issues related to inventory control will be follow-up audit priorities. Audit work will conclude with preparing another annual audit plan and the Annual Audit Report which will summarize all FY 2019 audit activity.

Risk information available at the time was considered in the preparation of this Plan, therefore, it is subject to revision should the risk climate materially change, or unexpected events occur. If this happens, the Director of Audits will promptly notify the Board and Executive Management of requested revisions to the Plan.

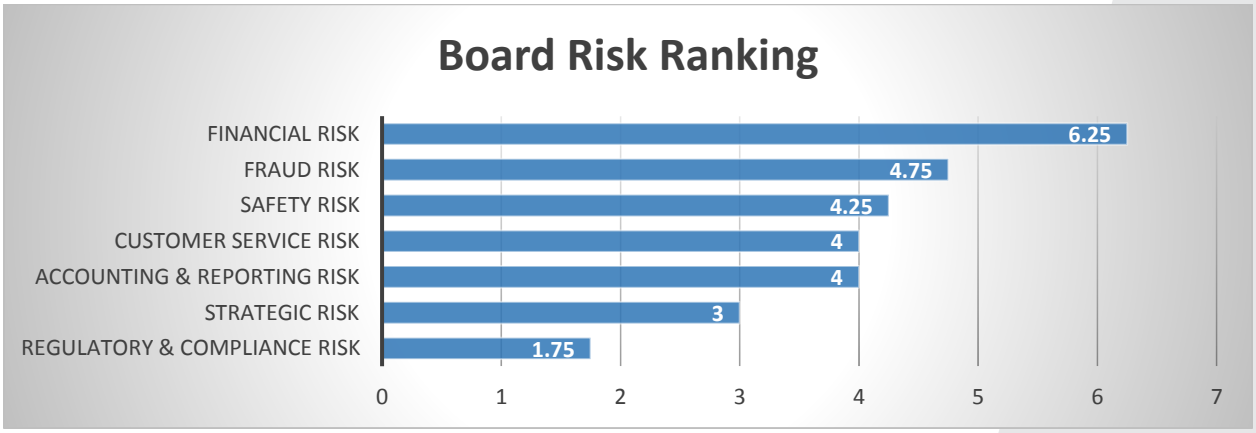
Description of the Risk-Based Methodology used to develop the Plan

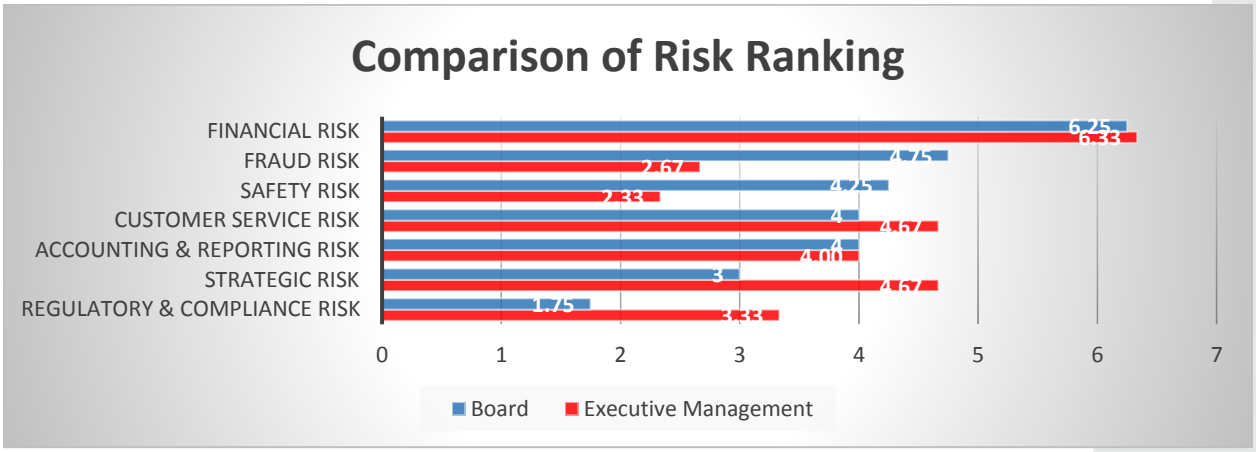
The planning process began with requesting input through a survey from the Board and Executive Management on their priorities related to the following 7 risks:

Strategic Risk
These are risks that will significantly reduce the likelihood that strategic goals and WIGS will be achieved.
Financial Risk

These are risks that will have significant financial impacts on the College. Consequences of these risks include important revenues being reduced or lost, or unnecessary expenses being realized.
Accounting & Reporting Risk
These risks affect key accounting records (financial statements, general ledger) and reports (reports sent to the Board, State, Feds), possibly causing them to be materially misstated.
Fraud Risk
These are risks that increase the likelihood that fraud, waste, and abuse occur within the organization.
Regulatory/Compliance Risk
These are risks of non-compliance to a significant statute, regulation, covenant, or policy the College is subject to.
Safety Risk
These are risks that increase the likelihood that a student, employee, or visitor of the College is seriously injured or killed.
Customer Service Risk
These risks significantly impact customers in a negative way. Examples include poor customer service, poor learning experience, missed deadlines on commitment, etc.

The results of that survey yielded the following results:





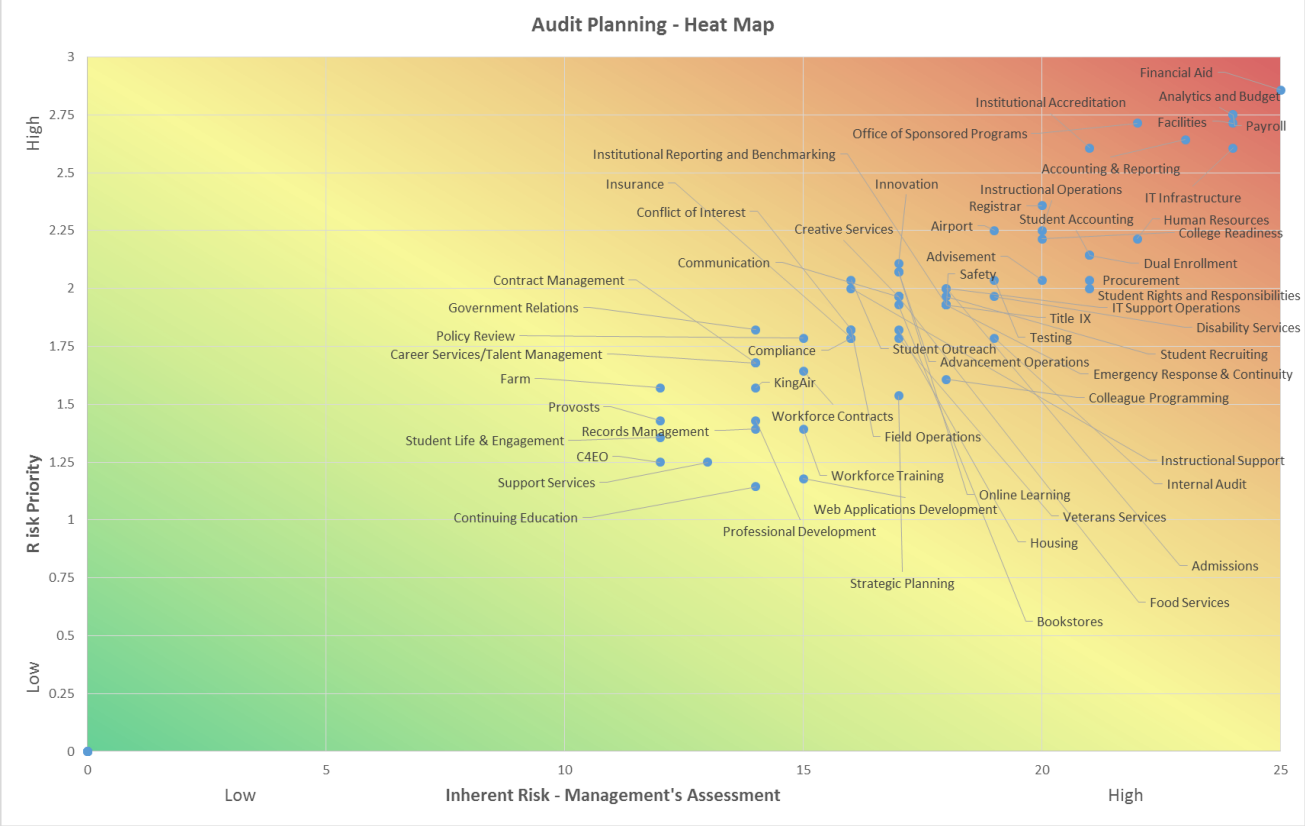
Using the results from the Combined Risk Ranking, each risk was assigned a weighted score based upon its position relative to the other risks. These weighted scores were then used in conjunction with scores from risk assessments performed by departmental managers (described

below) to determine the overall significance of activities and processes within the College relative to other activities.

Our next step was to solicit the opinion of departmental managers on how the risks impact their major activities and processes. This was achieved by requesting departmental managers rate the impact the individual risks would have on their areas if they materialized. Each risk carried the same weight. Their answers to each question were given raw scores and then summed for each activity being assessed.

The scores from the surveys answered by the Board and Executive Management along with the scores from the questions answered by departmental managers were plotted on the y and x axes, respectively, of a heat map to demonstrate the inherent risk each activity poses to the College.

Those results are as follows:



This heat map helped identify the activities and processes where audits would be most beneficial to the College.

Finally, we considered specific audit requests from all parties, as well as statutorily required audits. Those requests, with the exception of the required audits, are listed below. The frequency of a specific request is also listed. The indicates requests that are in some manner reflected in the Proposed Plan:

Governance	Safety/Active Shooter	Cybersecurity
C4EO	Technology	Strategic Plan Implementation
Human Resources	Title IX Compliance	Travel (2)
Industry Advisory Practices	Airport Operations	Workforce Training
Foundation Accounting	Graduation Process	TRS Contributions
Procurement Cards	IT Help Desk	GLBA Compliance
Cloud Security	Virtual Servers	Internet of Things
Software	Colleague (2)	Perceptive Content
Instructional Departments	Fleet	

Internal Audit Available Time

Total hours (5 Staff * 52 Weeks *40 hours)	10,400	100%
Less: Estimated vacation, holiday, sick, & training	1,720	17%
Total hours available for audits, other projects, & administration	8,680	83%

Total hours available for audits, other projects, & administration	8,680	100%
Less: Administration (meetings, travel time, research, campus volunteering, w/p reviews, campus education, etc)	2,130	25%
Total hours available for audits and risk based projects	6,550	75%

Description of Project Types

Full-scope audits: These are projects in which some activity or other management assertion is evaluated so that an objective opinion can be offered.

Follow-up audits: These are projects in which deficiencies identified in past audits are tested to ensure management applied appropriate corrective action, or has openly accepted the risk.

Risk assessments: These are consulting engagements in which Internal Audit facilitates a discussion with management to identify and document risks that are present in their areas of responsibility, and documents their assessment of how well those risks are currently mitigated.

Investigations: These are performed as a result of a complaint made either in person or anonymously through the College's or State Auditor's Office ethics hotlines. As a matter of rule, all complaints are investigated, with results communicated to the Board and other concerned parties.

Other projects: These include special projects requested by the Board or management, assistance given to external auditors, and administrative tasks within the Internal Audit such as preparing the annual audit plan, the Annual Audit Report, and staff evaluations.

Proposed Audit Plan

Risk Categories	FR	ARR	RCR	SR	FRR	CSR	STR	How selected?
Proposed Audits								
1. TEC 51.9337 (Contracting) Audit	■	■	■		■			Required annually
2. TAC 202 (IT Security) Audit			■		■	■		Required biennially
3. THECB Facilities Audit (West Texas)	■		■					Required every 5 years
4. THECB Facilities Audit (Marshall)	■		■					Required every 5 years
5. Integrated Admissions Process Audit	■			■		■		Risk based
6. TRS Contributions Audit	■	■	■			■		Risk based
7. Internal Penetration Test (North Texas)					■			Risk based
8. Internal Penetration Test (Ft. Bend)					■			Risk based
9. Google Drive Security Audit	■				■	■		Risk based
10. Workplace Harassment Audit			■			■	■	Risk based
11. Challenger Center Audit (Waco)	■			■		■	■	Risk based
12. Challenger Center Audit (Harlingen)	■			■		■	■	Risk based
13. Graduation Process Audit	■			■	■	■		Risk based
14. Maxient Software Audit					■	■	■	Risk based
15. C4EO Audit	■				■			Risk based

16. Fixed Asset Follow-up Audit								Risk based
17. Financial Aid Follow-up performed by State Auditor's Office						`		Required
18. Financial Statement Audit performed by independent CPA firm								Required by SACSCOC

FR - Financial Risk, **ARR** - Accounting Risk, **RCR** - Regulatory/Compliance Risk, **SR** – Strategic Risk, **FRR** - Fraud Risk, **CSR** - Customer Service Risk, **STR** - Safety Risk

	Audit will test specific risks in this category.

Descriptions of the projects follows:

1. TEC 51.9337 (Contracting) Audit: 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

2. TAC 202 (IT Security) Audit: This will be an audit of required IT controls. It will focus on the required IT control families listed in the regulation, with an emphasis on IT security.

3. THECB Facilities Audit (West Texas): This audit will test construction projects completed in West Texas between July 2013 and July 2018 to ensure they were properly reported to the THECB.

4. THECB Facilities Audit (Marshall): This audit will test construction projects completed in Marshall between July 2013 and July 2018 to ensure they were properly reported to the THECB.

5. Integrated Admissions Audit: This audit will test the effectiveness and efficiency of the admissions process to ensure potential students are being processed in a timely and effective manner to ensure maximum enrollment. Systems used in this process include Apply Texas and Sales Force. They will also be reviewed to ensure the information they provide is processed properly and securely.

6. TRS Contributions Audit: This audit will test TRS contributions. Areas that will be tested include report accuracy, employee elections and eligibility in TRS & ORP programs, contributions, and the employment of retirees.

7. Internal Penetration Test (North Texas): This will be a discreet unannounced attempt to inappropriately access IT hardware, software and other sensitive data and information through means available to the general public.

8. Internal Penetration Test (Ft. Bend): This will be a discreet unannounced attempt to inappropriately access IT hardware, software and other sensitive data and information through means available to the general public.

9. Google Drive Security Audit: This audit will test the administration of the Google Drive, and the security controls and processes that are in place.

10. Workplace Harassment Audit: This audit will test the policy and procedures relied upon to ensure various types of unlawful harassment are limited and appropriately handled when they occur.

11. Challenger Center Audit (Waco): This audit will test the effectiveness and efficiency of the Challenger Center operations in Waco.

12. Challenger Center Audit (Harlingen): This audit will test the effectiveness and efficiency of the Challenger Center operations in Harlingen.

13. Graduation Process: This audit will test the effectiveness and efficiency of the graduation process to ensure all graduates are eligible.

14. Maxient Software Audit: This audit will test the software used to track student discipline issues to ensure it is being utilized effectively, and in a secure manner.

15. C4EO Audit: This audit will test the accuracy of information related to C4EO reported to the Board on a quarterly basis.

16. Fixed Asset Follow-up Audit: This audit will test the accuracy and completeness of the annual inventory, updates to the fixed asset system, and improvements to the disposal process.

17. Financial Aid Follow-up Audit performed by the State Auditor's Office: The State Auditor's will follow-up on a deficiency identified on the Marshall Campus in 2014.

18. Financial Statement Audit performed by an independent public accounting firm: This audit will test the balances and assertions in the fiscal year end 2018 financial statements, as well as compliance to federal rules associated with federal awards. This is a required audit by SACSCOC. Audit delegation to hire an independent firm was received on March 30, 2018.

Texas State Technical College
Internal Audit
Status of Fiscal Year 2018 Audit Schedule & Other Projects

Description	Division/Campus	Status	Project No.	Report Date
INTERNAL AUDITS				
Public Funds Investment Act Audit	Financial Services	Complete	18-002A	9/1/17
Audit of Select Controls on Demand Deposits	Financial Services	Complete	18-002.1A	9/1/17
Departmental Audit - Industrial Maintenance	North Texas	Complete	18-011A	11/3/17
Departmental Audit - Provost Office	North Texas	Complete	18-010A	11/3/17
Facilities Development Project Compliance Audit	Facilities - Waco	Complete	18-019A	11/27/17
Evidence Room Audit	Waco & Harlingen Police Departments	Complete	18-021A	12/7/17
Review of Cohort Default Rate	Financial Aid	Complete	18-022A	12/12/17
Benefits Proportionality Internal Audit	Financial Services	Complete	18-018A	2/9/18
Departmental Audit - Provost Office	EWCHEC	Complete	18-024A	3/13/18
Departmental Audit - Welding	EWCHEC	Complete	18-025A	3/26/18
PCI Compliance Audit	Marketing/OIT	Complete	18-009A	5/14/18
Internal Penetration Test (Marshall)	OIT	Complete	18-026A	6/7/18
TEC §51.217 Safety Audit	Cross-Divisional	Complete	18-012A	6/11/18
TAC §202 Compliance Audit	OIT	Complete	18-003A	6/15/18
Fixed Assest Control Follow-up Audit	Cross-Divisional	Complete	18-037A	6/15/18
Internal Penetration Test (West Texas)	OIT	In Progress		
External Quality Assessment Review	Internal Audit	In Progress		
TEC §51.9337 Contracting Audit	Purchasing	In Progress		
Departmental Audit - Culinary Program	Waco	In Progress		
Departmental Audit - Culinary Program	Harlingen	In Progress		
EXTERNAL AUDITS				
Department of Education: Final Program Review Determination	Financial Aid	Complete		7/20/17
Workforce Solutions - Cameron County - Monitoring Review of Contract 2416 TCY2-00	College Readiness - Harlingen	Complete	18-008A	9/5/17

Description	Division/Campus	Status	Project No.	Report Date
THECB: Follow Up Audit of TEXAS Grant	Financial Aid	Complete		1/10/18
State Auditor's Office: Benefits Proportionality (2016 & 2017)	Financial Services	Complete		2/1/18
State Auditor's Office: A-133 Follow-up	Financial Aid - Harlingen	Complete		2/1/18
State Auditor's Office: A-133 Follow-up	Financial Aid - Marshall	Complete		2/1/18
THECB: TEOG Audit	Financial Aid	Complete		5/9/18
THECB: 2017/2018 Programmatic Desk Review of the Perkins Basic Grant - Report is final, response is being drafted.	Sponsored Programs	In Progress	18-023A	
State Comptroller's Office: Post Payment Audit	Purchasing	In Progress		

OTHER INTERNAL PROJECTS

Risk Assessment - Purchasing	Procurement	Complete	18-006RA	8/18/17
Re-calculation of Salaries - Workforce Development	Workforce Development	Complete	18-004P	8/23/17
Donation Process Review - Welding	Instructional -Brownwood	Complete	18-007I	10/9/17
SAO Hotline: Allegation of inappropriate purchasing and bonuses. Results: Conflict of interest procedures, as well as regulations governing merit increases and bonuses were followed. Found no evidence of fraud, waste or abuse.	Central Administration	Complete	18-015I	10/31/17
Internal Hotline: Allegation of employees abusing time. Results: Allegation was referred to individual supervisors to remind employees of College expectations if they were studying duirng working hours. The AVC stated she would require all VPSLs to remind faculty that work on their own studies must take place after working hours.	Instructional - Abilene	Complete	18-017I	11/17/17
SAO Hotline: Allegation that instructional quality in a program is poor because the former lead instructor was replaced. Results: Determined the allegation had no merit.	Instructional - Harlingen	Complete	18-020I	12/15/17

Description	Division/Campus	Status	Project No.	Report Date
Managemet Request: Reviewed a practice in which an internal report was being manipulated by inputing inaccurate processing codes for applications of potential students. Results: Determined the practice was based on a directive intended to make the report misleading. Also determined the practice resulted in untimely communication to applicants, and potentially erroneous external reporting.	Student Services	Complete	18-038I	3/27/18
Internal Hotline: Allegation that TGC 658.010 related to place of work is being violated when employees work at places other than their normal place of business. Referred to Human Resources. They interpretted the rule to require State business be conducted during normal business hours at the regular place of business or assigned duty point.	Human Resources	Complete	18-27I	4/25/18
SAO Hotline: Allegation that instructor is using college resources for personal benefit. Results: Determined that an instructor has brought his children to class on at least one occasion. We were unable to validate the allegation that personal work was being performed in the shop area, but confirmed that controls needed to be improved.	Instructional/Harlingen	Complete	18-042I	6/1/18
SAO Hotline: Allegation that a supervisor abuses time, misuses assets, and has an employee approve requisitions using the supervisor's credentials. Results: Determined that the requision allegation was legitimate. Was unable to verify the other allegations, but the employee was counseled on College expectations and requirements.	Student Development	Complete	18-045I	6/18/18
~~Business Process Risk Assessment~~	~~Ft. Bend~~	Requesting Removal		

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
PCI Compliance Audit (18-009)		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.	We determined that while the majority of the PCI DSS controls and control elements were implemented to ensure payment card data is secured, many required IT controls and control elements were still pending or needed improvement at the time of our testing. The detailed results of are testing has been made available to management to assist them in improving security and compliance.	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.	Herrera/LaForce	Aug-19

Report Name & No.		Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
				1.2 Several issues concerning storage of Credit Card information were noted. All units have been apprised of the standard and that practice has been discontinued. Going forward as part of our on site unit review/checklist, we will ensure the units are in compliance, as well to ensure that the retention schedule is being followed. There were several references to cashier training. We will create an in house training program. Format and parameters for that process are forthcoming.	Kilgore/Guercio	Aug-18

Report Name & No.		Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
Marshall: Internal Network Penetration Test (18-026A)		Physical and logical security could be improved by informing campus employees of the results of this project, and re-educating them on the risks we were able to exploit.	While many controls are in place, we did identify areas that need to be improved. The details of this finding are included in the Supplemental Audit Report rather than here so as to not create further risk. Please refer to that report for the support of this finding.	1.1 The TSTC Marshall Provost's Office has communicated the findings of the audit with all employees on the campus to provide awareness of the identified issues and improvements that can be made by everyone campus wide. The TSTC Marshall Provost's Office utilized the June 1st open forum as an opportunity for an open discussion of the findings. The Office of Information Technology will continue working with our Professional Development Department to provide ongoing yearly and periodic training to all employees to provide awareness of technology risks and how to protect the college.	Kilgore/Day	Jun-18
				1.2 The Office of Information Technology is currently in the process of implementing a centralized computer management solution, Microsoft Active Directory, which will enable us to implement technical controls to enforce security on workstations.	Herrera/Collatos	Dec-18

Report Name & No.		Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
				1.3 The Office of Information Technology is currently in the process of rolling out multifunction copiers and removing personal printers from workspaces. The use of multifunction copiers will enable employees to print securely while the printers are managed centrally. This will address the identified issues related to printers.	Herrera/Schulte	Jul-18
				1.4 The Office of Information Technology will evaluate additional security controls around network connectivity to address the identified issues, while still allowing productive access for students and employees.	Herrera/LaForce	Jul-18
Safety & Security Audit (18-012A)		Improvements should be made to standardize safety processes between campuses, and to better establish College expectations and accountability.	In addition to the specific safety deficiencies detailed in the confidential supplemental audit report, the following observations best illustrate the lack of standardized safety processes and understanding/accountability:	1.1 We are currently reviewing all safety processes, and will be standardizing them throughout the State. Our efforts will, at a minimum, address all observations noted in the audit report and include follow-up of the individual safety issues notes at each campus as detailed in the supplemental report. The revised processes will include a designated safety officer performing frequent inspections, along with training individual departments.	Herrera/ Shafer	Aug-19

Report Name & No.		Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
			* The responsibility to maintain the first aid kits is unclear to employees.			
			* Accident reporting and handling is inconsistent.			
			* Accident trend analysis is, at best, informal.			
			* The frequency, reliability, and type of safety inspections and safety drills differ between campuses.			
			* Safety related signage is outdated and inconsistent.			
			* Accountability for safety deficiencies is not well defined.			
			* Responsibilities and roles are defined differently from campus to campus.			
			* Certain safety controls, such as artificial defibrillator devices (AEDs) and emergency phones, are deployed differently on each campus.			
			* Annual tabletop exercises of the emergency operations plan are not performed at every campus.			

Report Name & No.		Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
TAC 202 Follow-up Audit (18-003A)		Forty one of 135 required IT controls were found to not yet be implemented.		1.1 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.	Herrera/LaForce	Ongoing
Fixed Asset Control Follow-up Audit (18-037A)		We identified processes that still require attention to ensure all assets are properly safeguarded after purchase.	For the 2017 annual inventory process, documentation was missing for some stewards which evidenced that their assets were inventoried. We also identified instances where changes/updates were notated by some stewards on their inventory forms, but asset records were not updated to reflect those changes.	All inventory asset control staff and directors had a training session with accounting and reporting staff where the team identified ways to ensure the inventory sheets are collected in full in the future. Management will going forward reconcile all stewards who need to complete annual inventory documentation to documentation that is actually received, and escalate the matter to appropriate management when reasonable follow-up requests with the employees do not work and/or proper documentation in the event of a form being turned in late or missing	Hoekstra/Anz	12/31/18

Report Name & No.		Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
			We identified some assets that were transferred from one steward to another without appropriate documentation being on file to indicate the receiving steward accepted responsibility for the asset.	We will also more closely monitor inventory forms being submitted, and update the fixed asset system to reflect all notations made by stewards. During our last audit we decided that we were going to transfer assets of employees leaving the college to the supervisor even when not signed within 2 weeks. While this seemed like a good business practice in theory, the reality was that we ended up with unsigned sheets. After reviewing that practice we decided to go back to getting signatures before transfer.		
			We identified some assets currently assigned to people who are no longer employed by the College.	Management well ensure that all transfers are supported by documentation signed by both the person releasing the asset and the person receiving it or in the case of employee separation, have the receiving steward acknowledge receiving the assets.Procurement will work together with Human Recourses to ensure that all assets are transferred to active employees during the campus clearing process to ensure accountability for missing items is assigned to the appropriate steward.		

Report Name & No.		Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
			For some assets coded as disposed, we were unable to determine where the assets actually went. And, based upon a review of records and observation of an asset in the warehouse, we determined that assets scheduled for disposal are sometimes coded as disposed prior to them actually being sold and removed.			

Final Report - A Compliance Desk Review of Texas Educational Opportunity Grant performed by the THECB		No findings noted.

Texas State Technical College
Internal Audit
Follow Up Schedule & Status

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
Harlingen, Waco, Marshall, WT, Sys Ops: 2014 Employee Time Reporting Audits, Hoekstra	1.	The forms used to report time should be enhanced to capture more information on the compensatory time that is being requested so as to assist HOD with verifying the time calculation. This would benefit employees by further ensuring they are credited with the correct amount of compensatory time.	1.2 HOD will review (and revise if necessary) all existing policies and procedures related to leave and compensatory time to ensure compensatory time is handled consistently throughout the System.	**Partially Complete:** HR personnel have been trained to better scrutinize all manual time sheets. In January 2016, an IT project was approved to create a single State-wide application to manage leave requests, accruals, and timesheets. This system will be computing device agnostic.	The new timekeeping system is due to Human Resources from the Programmers on 4/1/2018. Training will be completed in April and May. The new system will go live in May.	4/1/2018 - Pending Review
			1.3 Depending on availability of IT programming personnel, HOD will facilitate enhancements of the current leave system to accommodate automation of compensatory time recording and calculation.	See above.	See above.	4/1/2018 - Pending Review
			1.4 Once the method for time reporting is determined, System-wide training will be implemented.	See above.	See above.	4/1/2018 - Pending Review

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
Marshall: A-133 Audit (performed by the SAO), Herrera	1.	Summary: Cost of Attendance budgets need to be adjusted to reflect actual enrollment so that the potential for over awards is reduced.	The College is developing new procedures to prevent recurrence of the issue. New reports have been created and will be thoroughly tested during the Spring 2018 semester. While we do not anticipate a need to re-programming, we will request it. We anticipate the action to be complete by 01/31/18.	**Ongoing:** At 10/12/17, SAO performed follow-up testing and did not find any exceptions related to cost of attendance. However, they found one over award unrelated to COA, and elected to not remove the finding. At June 30, 2018, follow-up testing had begun.		2/1/19

Internal Network Penetration Test (16-016A), Herrera	1.	We were able to find information on the internet that was useful to us in our social engineering attacks. As such, we were able to obtain both end-user credentials to systems containing protected data, and other information that could be used to get those credentials using relatively low-tech methods. We also noted instances in which physical security needs to be improved. Finally, we were able to inappropriately access student and employee data on servers using techniques available to more sophisticated hackers.	We have reviewed the issues identified and agree that corrective actions are necessary. We formulated specific actions for each of the issues, and have already corrected some. All required actions will be completed no later than December 2016 since some actions will require assistance from personnel outside of OIT.	**Substantially Complete:** As of 7/7/17, 8 of 9 corrective action plans have been completed. The only item that is pending to be completed is CAP 2.1 relating to secured logons to lab computers. On 10/2/17, the Director of Cybersecurity indicated Dell One is being purchased which will resolve the remaining item. Expected completion date is being moved up from 8/31/19 to 8/31/18. On 1/4/18, we verified Dell One had been purchased, but not yet installed. On 6/11/18, we were informed that implementation would be pushed back to 12/31/18 rather than 8/31/18.	Per Director of CyberSecurity on 06/11/18, The Dell One implementation project is ongoing. We anticipate that we will have group policies and workstation authentication implemented and workstation rollout by December 2018.	12/31/18

Report Name & No., Resp. Sr Mgr		Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
Summary of Departmental Audits (Marshall Welding Department 17-013A, Fort Bend Diesel 17-023A, Fort Bend HVAC 17-022A), Hoekstra	1.	We identified numerous exceptions related to inventory control in the Welding Department.	1.1 Summary : Create a cross-divisional team and review existing policies and procedures related to the inventory process.	**Ongoing:** We completed a follow-up audit in June 2018, and determined that process related to the safeguarding of assets still needed to be improved. Procedures related to terminated employees and disposal of assets were the primary areas that need attention.		8/31/19
TAC §202 Compliance Audit (17-002A), Herrera	1.	Twenty-three of the 106 IT controls we tested have not yet been implemented.	As noted in the report, a majority of the required controls have been implemented with the remaining controls being evaluated and addressed. For the controls not yet implemented, we are evaluating the associated risk to TSTC and associated applicability in our environment to prioritize implementation. IT Security along with TAC 202 compliance is a priority for TSTC.	**Ongoing:** As of 5/31/18, Internal Audit determined that efforts were still ongoing to implement all missing controls. The biennial audit will be performed in FY 2019 in which progress on missing controls, and status of implemented controls will be re-verified.		TBD

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
Annual Compliance Audit of TEC §51.9337 (17-028A, Hoekstra & Rushing	1.	A single contracting policy noting specific requirements of TEC §51.9337 still needs to be created, and subsequently adopted by the Board of Regents.	1.1 A contract management handbook, contract delegation of authority guidelines, and training protocols have been developed with assistance from our Office of General Counsel. A Statewide Operating Standard on contract management will be developed and presented to the Board for approval at their February meeting. This Contract Management SOS will contain delegation of authority protocols that will supersede all other delegations of authority included in existing SOSs.	**Pending Review:** As of 3/28/18, a proposed Contract Administration SOS had been created, but revised due to changes in the SOS format. Currently, all pending SOS's are on hold due to further changes in the SOS process. As of right now, an expected completion date is unknown. Internal Audit is currently performing the full-scope annual audit.		TBD
			1.2 The delegation of authority language included in existing SOSs will be removed as each SOSs is reviewed during the normal course of business.	**Pending Review:** As of 3/28/18, The contract compliance manager has reportedly reviewed the SOSs included on the Delegation of Authority. We are in the process of verifying if any changes were actually made. Internal Audit is currently performing the full-scope annual audit.		TBD

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.	Exceptions related to training, contract risk analysis, contract execution by unauthorized individuals, and other documentation exceptions indicate some of the requirements have not yet been fully implemented.	2.1 In FY2016 all employees with delegated authority to execute contracts were trained on contract management procedures. In FY2017, several training sessions were conducted; however, these were not mandatory and we didn't achieve 100% participation. Although Senate Bill 20 does not specifically set the frequency for contract related training, we agree with the recommendation to offer this training on an annual basis and to make it a mandatory training for employees with delegated authority to execute contracts. With assistance from Professional Development Office, work is already underway to develop a training module available via our LMS. Training for the Board will also be developed.	**Pending Review:** As of 3/28/18, training for the BOR or others delegated to approve contracts has not yet occurred. Department has been in communication with Professional Development to determine the best format to issue the training. Additionally, training has been delayed due to enhancements to the contracting process (recently adding a new project manager to be the starting point for all contracts). Internal Audit is currently performing the full-scope annual audit.		8/31/18
			2.2 A formal risk analysis procedure will be developed and implemented.	**Pending Review:** As of 3/28/18, a formal risk analysis process has been included in the SOS mentioned in CAP 1.1. It has yet to be implemented. Internal Audit is currently performing the full-scope annual audit.		TBD

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
			2.3 Delegation of authority guidelines will be covered during the annual mandated contract management training, general procurement training, and by email to all employees when the SOS on Contract Management is approved.	**Pending Review:** As of 3/28/18, training for the BOR or others delegated to approve contracts has not yet occurred. Department has been in communication with Professional Development to determine the best format to issue the training. Additionally, training has been delayed due to enhancements to the contracting process (recently adding a new project manager to be the starting point for all contracts). Internal Audit is currently performing the full-scope annual audit.		8/31/18
Departmental Audit of EWCHEC Welding (18-025A), Stuckly, Hoekstra	1.	Procedures related to sick leave needs to be improved to ensure related use is in compliance with College policy.	1.1 The Production and Manufacturing Division Director will ensure compliance with Texas State Technical College Policy and accepts the findings in this report. Training on leave policies will be provided to the department in coordination with Human Resources and any required corrective actions related to this finding will be taken. This will assure the EWC Welding Department conforms with our policies.	**Pending Review:** Internal Audit will review sick leave usage in October 2018.		Immediately

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
Application Process Investigation (18-038I), Herrera	1.	Summary: Admissions procedures need to be improved to ensure all applicants receive timely communication, and to ensure all internal and external reporting is accurate.	1.1 The work performed by the Internal Audit Department further justifies our movement towards a centralized processing center where stricter internal controls and monitoring can take place. The recommendations for improvement are areas in which we are working to address.	**Ongoing:** Internal Audit will perform a full scope audit of the admissions process in Spring 2019.		Immediately
PCI Compliance Audit (18-009A), Herrera, Kilgore	1.	Numerous IT related controls and/or their control elements, as prescribed by PCI DSS, have not been implemented. As such, PCI DSS compliance is not being fully met.	1.1 In an effort to ensure the protection of payment card data for students and employees, The Office of Information Technology has been working with Food Services to resolve a number of important control deficiencies during the audit and will continue to review and implement recommendations moving forward. As we anticipate that the review and implementation review of 100 controls across 6 objectives will take over a year, we will prioritize controls that have the largest impact on the protection of cardholder data. As part of this process, we will also implement the recommendation of an annual assessment of PCI-DSS controls to ensure ongoing adherence to PCI-DSS compliance changes.	**Ongoing**		8/31/19

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 Several issues concerning storage of Credit Card information were noted. All units have been apprised of the standard and that practice has been discontinued. Going forward as part of our on site unit review/checklist, we will ensure the units are in compliance, as well to ensure that the retention schedule is being followed. There were several references to cashier training. We will create an in house training program. Format and parameters for that process are forthcoming.	**Ongoing**		8/31/18

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
Marshall: Internal Network Penetration Test (18-026A), Herrera, Kilgore	1.	Physical and logical security could be improved by informing campus employees of the results of this project, and re-educating them on the risks we were able to exploit.	1.1 The TSTC Marshall Provost's Office has communicated the findings of the audit with all employees on the campus to provide awareness of the identified issues and improvements that can be made by everyone campus wide. The TSTC Marshall Provost's Office utilized the June 1st open forum as an opportunity for an open discussion of the findings. The Office of Information Technology will continue working with our Professional Development Department to provide ongoing yearly and periodic training to all employees to provide awareness of technology risks and how to protect the college.	**Pending Review**		Immediately
			1.2 The Office of Information Technology is currently in the process of implementing a centralized computer management solution, Microsoft Active Directory, which will enable us to implement technical controls to enforce security on workstations.	**Ongoing**		12/31/18

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
			1.3 The Office of Information Technology is currently in the process of rolling out multifunction copiers and removing personal printers from workspaces. The use of multifunction copiers will enable employees to print securely while the printers are managed centrally. This will address the identified issues related to printers.	**Ongoing**		7/31/18
			1.4 The Office of Information Technology will evaluate additional security controls around network connectivity to address the identified issues, while still allowing productive access for students and employees.	**Ongoing**		7/31/18
Safety & Security Audit (18-012A), Herrera	1.	Improvements should be made to standardize safety processes between campuses, and to better establish College expectations and accountability.	1.1 We are currently reviewing all safety processes, and will be standardizing them throughout the State. Our efforts will, at a minimum, address all observations noted in the audit report and include follow-up of the individual safety issues notes at each campus as detailed in the supplemental report. The revised processes will include a designated safety officer performing frequent inspections, along with training individual departments.	**Ongoing**		8/31/19

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
Harlingen: Automotive Program Investigation (18-042I), Stuckly	1.	Assets within the Automotive Instriction Program in Harlingen need to be better controlled.	1.1 A formal process is established and listed in the department "Rules & Regulations" document that includes a "live work" policy listing the criteria for accepting vehicle projects as part of the learning process and delivery of instruction.	**Pending Review:** We will review in Fall 2018.		Immediately
			1.2 It is the responsibility of the departments' faculty & instructional staff to ensure that all projects in the laboratory have a completed and signed repair order.	**Pending Review:** We will review in Fall 2018.		Immediately
			1.3 Any vehicle donated to the department for instructional purposes will be processed & reported through the TSTC Foundation Office and inventoried for stewardship in accordance with college policy. The department is to obtain proper documentation and forward to perspective offices in compliance of records management.	**Pending Review:** We will review in Fall 2018.		Immediately
			1.4 Agreements for loaner vehicles from manufacturer are submitted through the college legal counsel office for review, acceptance and signatures in accordance with policy.	**Pending Review:** We will review in Fall 2018.		Immediately

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
			1.5 Faculty and instructional staff are responsible for keeping the laboratory vehicle storage yard area locked at all times and continue to closely monitor the area for any unauthorized access by visitors, college students from other departments or anyone not in official business with the department.	**Pending Review:** We will review in Fall 2018.		Immediately
Harlingen: Disability Services Investigation (18-045I), Herrera	1.	Supervisor shared her password with another employee so to approve requisitions.	1.1 Vice President counseled the employee on sharing passwords being a policy violation and security issue, and instructed her to change the password(s).	**Pending Review:** We will review change logs to determine whether all Colleague passwords have been changed. We will also attempt to review REQM approvals to determine whether requisitions were approved by the same person who was logged into Colleague.		Immediately
		Data usage for a mobile hotspot was high.	1.2 Vice President counseled the employee on utilizing college resources for legitimate business. No evidence was found to conclusively prove the hotspot was ever used inappropriately.	**Pending Review:** In Fall 2018, we will again review data usage for the device and attempt to determine who used the device.		Immediately

Internal Audit Department

Audit Report

Payment Card Industry (PCI) Data Security Standard Audit (18-009A)

TEXAS STATE TECHNICAL COLLEGE

May 14, 2018

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 payment card security as of March 31, 2018. This internal audit was to assess the College's compliance to the data security standards (PCI DSS) set forth by the PCI Security Standards Council to ensure payment cards are handled and processed in a safe and secure manner to limit unauthorized access to sensitive information tied to the cards. PCI DSS specifies minimum controls for protecting payment card data, and applies to all companies who receive, process, or transmit payment card data.

The College has three primary business units that accept payment cards (aka credit cards). Those units include the cafeterias, all bookstores, and the cashier's offices where payments are made on student and other accounts. Because the Harlingen and Waco cafeterias account for the majority of payment card volume at the College, the scope of this audit only included controls at these cafeterias. Nevertheless, Several IT controls we tested still apply to the other business units because they are either policy focused, or are also relied upon by those other units.

PCI DSS has six primary objectives that include twelve basic requirements. Those requirements include 267 prescriptive controls and control elements that apply to the cafeterias. We tested all applicable controls and control elements in this audit. The following matrix summarizes the results of our testing.

Objective 1: Build and maintain a secure network and systems.	
1. Install and maintain a firewall configuration to protect cardholder data.	**2. Do not use vendor-supplied defaults for system passwords and other security parameters.**
Objective 1 Conclusion: A secure network and related system has generally been implemented within the cafeterias. To improve this security, formal configuration standards should be developed and implemented for firewalls, routers, and the system that is used. Also, inbound traffic should be limited to a DMZ.	

Objective 2: Protect cardholder data.	
3. Protect stored cardholder data.	**4. Encrypt transmissions of cardholder data across open, public networks.**
Objective 2 Conclusion: Sensitive cardholder data is not stored, and is encrypted during transmission. The policies related to security and data retention need to address card holder data.	

Objective 3: Maintain a vulnerability management program.	
5. Protect all systems against malware and regularly update anti-virus software or programs.	**6. Develop and maintain secure systems and applications.**
Objective 3 Conclusion: There is a vulnerability management program in place for the cardholder environment in the cafeterias, but anti-virus logs are not maintained for the required length of time. We also found some computers with outdated anti-virus software, and prior to March 2018, external vulnerability scans were not performed by a PCI approved vendor.	

Objective 4: Implement strong access control measures.	
7. Restrict access to cardholder data by business need to know.	**8. Identify and authenticate access to system components**
9. Restrict access to cardholder data by business need to know.	
Objective 4 Conclusion: Strong access controls have generally been implemented, but need to be strengthened. We found accounts that needed to be revoked or changed, visitor log in the datacenter not always completed, password changes after first logon are not enforced, and the security policy and training of people who handle cards needing to be improved.	

Objective 5: Regularly monitor and test networks.	
10. Track and monitor all access to network resources and cardholder data.	**11. Regularly test security systems and processes.**
Objective 5 Conclusion: Monitoring capabilities exist for the payment card environment, however, security would be improved by actively reviewing audit logs other than on an exception only basis, performing internal vulnerability scans on a more frequent basis, continuing to have external vulnerability scans performed by a PCI approved vendors, and scanning the payment card environment quarterly for unauthorized wireless access points.	

Objective 6: Maintain an information security policy.
12. Maintain a policy that addresses information security for all personnel.
Objective 6 Conclusion: A security policy and related procedures have been implemented. As previously alluded to though, it is missing specific language related to payment cards.

We determined that payment card security in the cafeterias is generally well controlled, but is not yet fully complying with data security standards set forth by the PCI Security Standards Council. Many key controls are in place, but because PCI DSS is so prescriptive, there are elements of the controls that need to be enhanced. To assist management with

those efforts, we developed a detailed document which outlines the specific controls and control elements that either have been implemented or needs improvement. The controls relied upon by the bookstores and cashier's offices for payment card security will also be improved by addressing the areas we identified needing improvement in this audit.

Introduction

The cafeterias on the Harlingen and Waco campuses accepted approximately 33 thousand and 30 thousand payments, respectively, from payment cards issued by Visa, Mastercard, Discover, and American Express from September 1, 2016, through July 31, 2017. Both cafeterias use the Micros Res application (aka Oracle Hospitality Res), a validated payment application that has been independently assessed for compliance with the Payment Application Data Security Standard (PA-DSS). Through Micros Res, the cafeterias receive point-to-point encryption from Merchant Link for payments they receive using payment cards. Merchant Link is also an approved PCI-compliant service provider. Merchant Link partnered with Micros Res to develop an integrated solution that encrypts sensitive card data at the swipe on workstations or via external card readers.

PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data and/or sensitive authentication data. PCI DSS includes 351 controls and control elements, with 267 being applicable to the cafeterias at the College.

PCI DSS compliance and payment card security are affected by how payment cards are handled in each business unit, by the software and hardware utilized to receive payments via cards, and by other controls managed within the Office of Information Technology (OIT). Risks could materialize through low tech means such as a cashier writing down payment card account numbers, or through more sophisticated hacking attempts. Accordingly, the risks must be managed through a collaborative approach, with some being handled within the business units and others within OIT. Stated simply, effective payment card security is dependent upon manual and automated controls.

Objectives

The primary purpose of the audit was to ensure payment cards accepted by the cafeterias are handled and processed in a safe and secure manner to limit unauthorized access to sensitive cardholder information. To do this, we verified the minimally required PCI DSS security processes and controls have been implemented as required by the Payment Card Industry Data Security Standard (PCI DSS).

Scope & Methodology

The scope of our audit included all automated and manual controls related to payment cards that are managed by the cafeteria and/or OIT for the cafeterias on the Harlingen and Waco campuses. All applicable controls required by PCI DSS were tested. We utilized the following documents to test the required controls:

- the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures Version 3.2 dated April 2016, as well as the PCI DSS Self-Assessment Questionnaire (SAQ - D) and the SAQ Instructions and Guidelines,
- the Attestation of Compliance for Merchants Revision 1.1 dated January 2017,
- the PCI DSS Quick Reference Guide,
- the PCI DSS Glossary of Terms, Abbreviations, and Acronyms,
- the Prioritized Approached for PCI DSS,
- the PCI for Small Merchants website,
- the PCI Frequently Asked Questions,
- the lists of Approved Scanning Vendors (ASVs) and PA-DSS validated payment applications,
- and various supporting resources and best practices described at the PCI Security Standards Council Website and document library.

General Observation

We determined the majority of the required PCI DSS controls have been implemented. In this project, we worked closely with OIT and cafeteria personnel. The PCI DSS mandates are a challenging undertaking for most organizations. Nevertheless, OIT and cafeteria staff are diligently trying to implement all controls. Everyone we worked with was receptive to our observations and recommendations, and immediately started to close gaps as we identified them.

Summary of Finding

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.

Opinion

Based on the audit work performed, we determined that payment card security in the cafeterias is generally well controlled, but full compliance with the data security standards set forth by the PCI Security Standards Council has not been met. While many key controls are in place, there are elements of the controls that need to be enhanced. We would like to express our gratitude for the time and assistance provided by the staff during this audit.

Submitted by:

Jason D. Mallory, CPA, CIA	May 14, 2018 Date

AUDIT FINDING DETAIL

Finding #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.

Criterion: The PCI Data Security Standard Requirements specify the minimum information security controls to implement to ensure payment card information is secured. Security Assessment Procedures specify the testing procedures to validate whether those controls have been effectively implemented. For each required control, we reviewed formal policies and procedures, validated system configurations, verified various information system functions and processes, and inquired of numerous other controls. We also examined related documents and system generated reports/screenshots to determine whether controls were implemented.

We determined that while the majority of the PCI DSS controls and control elements were implemented to ensure payment card data is secured, many required IT controls and control elements were still pending or needed improvement at the time of our testing. The detailed results of are testing has been made available to management to assist them in improving security and compliance. They are not detailed in this document due to the potential sensitivity.

Consequences: A security breach and subsequent compromise of payment card data has far-reaching consequences for affected organizations. Those could include regulatory notification requirements, reputational impact, potential financial liabilities (regulatory and other fees and fines), and litigation.

.

Possible Solution: We recommend the results from this audit be utilized to improve overall PCI DSS compliance in all business units that handle payment cards. We also recommend an annual risk assessment be performed by management, with periodic internal audits to validate their self-assessment.

Management Response:

Division: Office of Information Technology
Senior Management: Ricardo Herrera, Chief Technology Officer
Jeff Kilgore, Chief Marketing Officer

Task	Brief Description	Responsible Individual	Completion Date
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	Donald Laforce, Greg Guercio	8/31/2019

	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.		
1.2	Several issues concerning storage of Credit Card information were noted. All units have been apprised of the standard and that practice has been discontinued. Going forward as part of our on site unit review/checklist, we will ensure the units are in compliance, as well to ensure that the retention schedule is being followed. There were several reference to cashier training, We will create an in house training program. Format and parameters for that process are forthcoming.	Greg Guercio	12/31/18

Internal Audit Department

Audit Report

Internal Network Penetration Test Audit (18-026A)

TEXAS STATE TECHNICAL COLLEGE

Marshall Campus

June 7, 2018

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 March 26 and April 18 2018, we performed vulnerability scans and penetration testing of the College's internal network on the Marshall 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 campus. Physical and logical security controls, to include the actions and habits of personnel, were targeted in this project. We specifically focused on likely attack vectors that could be exploited by bad actors to gain unauthorized access to sensitive information and information technology assets.

The scope of the penetration test included the physical and logical securities of core network equipment and servers located on the Marshall campus. We approached the test from the perspective of an unauthorized individual with limited knowledge of available assets and controls. To gain an understanding, we relied upon information available to the general public by performing internet searches and physically observing facilities to identify potential weaknesses. We tested end user training effectiveness (known as phishing) by calling and sending emails to select individuals requesting sensitive information that would never legitimately be sought. We attempted to access areas that should be restricted to determine what sensitive information or assets we could likely pilfer. And we attempted to gain access to privileged systems and information by scanning the network to identify control flaws, testing wireless access, and searching for available ports that we could plug into. Finally, we accessed computers available to the public to determine whether we could gain access to sensitive information. Both manual and automated testing methods were used to detect and/or exploit vulnerabilities. Industry standards noted in the Scope & Methodology section of this report served as our basis.

We determined that employees are generally vigilant in protecting sensitive information during social engineering attempts, do not generally expose sensitive information by disposing of documents within recycle/trash bins or leave documents in public view, and use password protected screensavers on their machines when they are not at their desks. Some employees did report our phishing attempts, and the IT Help Desk has established protocols for notifying the campus of current attacks to minimize success. We verified that wireless access signals are confined to the campus, guest networks are segregated from internal networks, and access to internal networks and systems are protected through secured logon protocols and encryption. We also found that access to server rooms was restricted by electronic locks that required a PIN and badge. Finally, IT personnel were unwilling to change passwords to systems without first verifying our actual identity.

While not widespread, we were able to gain access to the Colleague system through our phishing techniques, found instances where assets and information was not appropriately safeguarded by end users, and was able to scan the network from within a study room within the library without

signing in to the library. Most of the vulnerabilities we identified in this project were the result of employees (non-IT) not following established protocols. Accordingly, we feel most of the gaps we identified could be easily resolved by informing the campus community of this project and its results, and re-educating employees on the risks they must help control. A confidential supplemental report is available describing the specific vulnerabilities we identified that need to be addressed.

Introduction

The Office of Information Technology (OIT) Division, directed by the Vice Chancellor/Chief Technology Officer, consists of 3 departments – the IT Support Operations Department with a staff of 45, the Department of Infrastructure Operations with a staff of 22, and the Department of Cyber Security with a staff of 1. OIT 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.

During this internal penetration test Internal Audit worked closely directly with the Director of Cybersecurity. Members of the IT Support Operations Department and the Department of Infrastructure Operations were only notified when accounts were compromised or immediate remediation was required. To ensure the integrity of the results, limited people were notified of our tests prior to us performing them.

Network penetration tests simulated attempts to access and/or disrupt IT operations and assets with the ultimate goal of obtaining sensitive information. In FY 2015, an external test was performed which simulated attacks from off-campus sites through the internet by a consultant. The internal test performed in this project simulated on-campus attacks by exploiting risks identified through first hand observations.

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 test all risks the campus is subject to during an attack. We focused on likely scenarios based upon the information we gathered during our testing.

Scope & Methodology

The scope of the penetration test included the physical and logical securities of core network equipment, access network equipment, and servers located on the Marshall campus. 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

General Observations

Physical and logical access was generally secured. Server rooms and other rooms and closets storing network hardware were locked during testing. Help Desk personnel utilized a robust procedure requiring call backs to verify identities before changing passwords. Most employees were unwilling to disclose personal information and passwords, and OIT was responsive to known attacks. Wired and wireless networks are segregated between privileged and guest accounts, with services being appropriate on each. Logon credentials are required to access both the secured network, and the various services on it. Wireless access points are unlikely to emit signals that can be used by bad actors outside of the physical perimeters of the originating buildings. The physical security of administrative offices were generally monitored and restricted.

Summary of Findings

Physical and logical security could be improved by informing campus employees of the results of this project, and re-educating them on the risks we were able to exploit.

Opinion

Based on the audit work performed, IT assets and information are generally well protected, but specific instances of physical and logical security need to be improved. A confidential supplemental report is available describing the specific vulnerabilities that need to be addressed.

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

Submitted by:

	June 7, 2018
Jason D. Mallory, CPA, CIA	Date

AUDIT FINDING DETAIL

Finding #1: Physical and logical security could be improved by informing campus employees of the results of this project, and re-educating them on the risks we were able to exploit.

Criterion: Posing as a student, we walked through various buildings on each campus during and after business hours. We attempted to access buildings and rooms that contained IT equipment and potentially sensitive information. We took note whether people or other obstacles prevented access. We also made phishing telephone calls and sent emails to employees in an attempt to learn logon IDs and passwords. And we scanned the network searching for vulnerabilities that could potentially be exploited. Finally, we attempted to access privileged areas via wireless access.

While many controls are in place, we did identify areas that need to be improved. The details of this finding are included in the Supplemental Audit Report rather than here so as to not create further risk. Please refer to that report for the support of this finding.

Consequences: Failure to address the vulnerabilities exposes sensitive information to unauthorized access, and equipment to theft.

Possible Solution: We recommend all campus employees be informed of our project results, and everyone be reminded of their responsibilities to protect sensitive information and IT assets.

Management Response:

Division: Office of Information Technology
Senior Management: Ricardo Herrera

Task	Brief Description	Responsible Individual	Completion Date
1.1 Personnel Security	The TSTC Marshall Provost's Office has communicated the findings of the audit with all employees on the campus to provide awareness of the identified issues and improvements that can be made by everyone campus wide. The TSTC Marshall Provost's Office utilized the June 1st open forum as an opportunity for an open discussion of the findings. The Office of Information Technology will continue working with our Professional Development Department to	Bart Day	Completed 6/1/18

Task	Brief Description	Responsible Individual	Completion Date
	provide ongoing yearly and periodic training to all employees to provide awareness of technology risks and how to protect the college.		
1.2 Workstation Security	The Office of Information Technology is currently in the process of implementing a centralized computer management solution, Microsoft Active Directory, which will enable us to implement technical controls to enforce security on workstations.	Richard Collatos	12/31/18
1.3 Printer Security	The Office of Information Technology is currently in the process of rolling out multifunction copiers and removing personal printers from workspaces. The use of multifunction copiers will enable employees to print securely while the printers are managed centrally. This will address the identified issues related to printers. Rollout of multifunction copiers is completed.	Jill Schulte	7/31/18
1.4 Network Security	The Office of Information Technology will evaluate additional security controls around network connectivity to address the identified issues, while still allowing productive access for students and employees	Donald LaForce	7/31/18

Internal Audit Department

Audit Report

Safety & Security Audit (18-012A)

TEXAS STATE TECHNICAL COLLEGE

June 11, 2018

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 safety and security processes at the College as of March 31, 2018. Texas Education Code §51.217 requires an audit at least every three years of the safety and security of the institution's facilities. Given the sensitivity of the subject, the results are not subject to disclosure under Texas Government Code, Chapter 552, commonly referred to as the Public Information Act. As such, detailed issues are cited in a supplemental report. We last performed this audit in fiscal year 2015.

While we performed tests and observations at every campus, our primary focus was on the College's overall process of safety and security which ensures students, employees and other resources are safe on a continual basis. Our audit utilized select checklists developed by the Texas School Safety Center at Texas State University, and included tests to verify the following at each campus:

- Police and/or security presence, to include required training.
- Actions taken on, and communication of, observations made during previous inspections by the Fire Marshal, State Office of Risk Management, and Internal Audit.
- Implementation of safety controls at select buildings on each campus based upon on-site inspections.
- Periodic self-inspections by designated safety personnel.
- Periodic fire drills and related controls such as operational fire extinguishers, fire alarms, and sprinkler systems.
- Implementation and effectiveness of the emergency alert system.
- Food handling safety, where applicable.
- Safety related training.
- Emergency Operations Plan, and annual testing.
- Accident reporting and handling.

We determined that every campus has generally implemented safety controls that reasonably protect the well-being of students, employees and other assets. A few common ones include fire alarms, extinguishers and periodic drills, oversight and use of personal protective equipment in student labs, well-maintained facilities, implementation of an emergency alert system, and designation of safety personnel. A more detailed list for each campus is included in the Positive Observations section of this report. We also identified during our on-site inspections several safety lapses at each campus. These were immediately communicated to the respective safety representatives and Provosts for action. These observations are included in a separate, confidential supplemental report.

We determined that safety and security is a priority at each campus, and the College is generally safe. But, there are improvements that need to be made to standardize safety processes between campuses, and to better establish College expectations and accountability. During the course of this audit, we spoke to Executive Management,

Provosts, and safety personnel about our concerns, and they immediately began implementing improvements. Their plan is discussed in more detail in the management response section of the Finding #1 at the end of this report.

Introduction

The College has ten campuses throughout the state that are comprised of over 120 educational and administrative structures, 50 group housing structures, 14 athletic facilities and fields, and hundreds of houses and duplexes (on the Waco campus). These structures sit on approximately 3,000 acres of land. The College also owns agricultural property used for those purposes, and a large airport that accommodates tens of thousands of flights annually. Educational programs taught by the College include courses related to computers, flight instruction, light and heavy equipment repair, welding, machining, and construction. Each program has its own risk profile. The College also has over 1,500 employees that engage in instruction, administration, facilities maintenance and repair, law enforcement, and various customer service roles (i.e., food service, cashiers, retail operations). There are countless safety risk exposures, with common ones being associated with student and employee injuries, criminal activity, natural disasters, and vehicle and airplane crashes. Past injuries have included cuts, burns, crushes, sprains, and breaks due to accidents and carelessness. Crimes included thefts, aggravated assault, theft, and sexual assaults. The campuses have also been exposed to tornadoes, wind and hail damage, hurricanes, floods, and fires. These all remain probable risks.

The College has adopted a multi-layered approach in achieving safety and security. This approach encompasses student and employee well-being, as well as limiting the financial exposure associated with damage and loss of assets. Controls such as periodic self-inspections and inspections by outside agencies, comprehensive policies and procedures adopted by the Board of Regents, insurance, designated safety personnel, and various facility controls have been implemented.

A Safety Department currently compromised of two full-time safety officers, stationed on the Harlingen and Waco campuses, provide safety guidance to all campuses. They also perform safety inspections on a limited basis, facilitate annual inspections of fire alarms, extinguishers, and sprinkler systems, and conduct safety training. The other campuses have designated safety coordinators who receive a monthly additional duty stipend to perform tasks similar those mentioned above, except on a reduced basis.

Objectives

The objectives of this audit were to ensure that the College has implemented safety and security processes that protect people and assets, and, on a sample basis, to identify any current deficiencies that need to be corrected. This audit is intended to satisfy the 3 year audit requirement of Texas Education Code §51.217.

Scope & Methodology

The scope of our audit included various personal and property safety and security risks at all 10 campuses within the College through March 31, 2018. To accomplish our audit objectives, we reviewed safety and security policies and procedures at each campus, performed on-site inspections on a sample of facilities, reviewed accident and self-inspection reports, interviewed numerous personnel, and reviewed other documents and procedures. We also utilized checklists published by the Texas School Safety Center, and reviewed inspection reports provided by the State Office of Risk Management and the State Fire Marshal.

Positive Observations

Safety and security are primary concerns at the College, and was evident throughout our audit. We made the following positive observations which reflect the efforts and resources being directed towards these endeavors.

All Campuses

- An emergency communications system has been implemented which uses text messaging, e-mails, and phone calls to alert employees and students of emergency situations. People must opt out from receiving the communications. This system is regularly tested.
- Comprehensive safety related policies are in place. Some of the more extensive ones include a Business Continuity Plan, Emergency Operations Plan, Sexual Assault and Harassment Policies, Personal Protective Equipment Policy, and a policy on the Campus Security Act.
- An Annual Security Report is prepared and published that informs concerned people of specific crimes that occurred on each campus.
- Safety Data Sheets are maintained of chemicals that are stored on campus, and we did not identify any stockpiles of unused chemicals.
- Facilities are generally well-maintained, and each campus has personnel dedicated towards this goal.
- Fire extinguishers, alarms, artificial defibrillator devices, and first aid kits are deployed throughout each campus.
- Instructors actively oversee student labs, provide program specific safety training, and generally enforce personal protective equipment requirements.
- Each campus has a safety representative.
- Almost all prior internal audit deficiencies were corrected, with no evidence of recurrence.
- There is a defined process for accident reporting and handling.
- Fire drills are periodically performed on at each campus.
- Landscaping and outdoor lighting limit blind spots and dark areas.

- Executive Management and the Board of Regents have established an expectation of safety and security.
- There is a Safety Department that provides guidance.
- There are dedicated student disciplinary procedures and personnel, with specific procedures for compliance to Title IX and VAWA regulations.
- There is a culture of zero tolerance for harassment and/or bullying of any kind, with recent examples of enforcement being available.

Abilene Campus

- Full-time police officer on duty.
- Quarterly building inspections are performed consistently.
- Additional duty safety officer participated in monthly safety meetings between West Texas campuses.
- Cafeteria received an excellent grade on recent food handling inspection.
- Limited accidents occurring on campus.
- Periodic inspections by the State Office of Risk Management and the Fire Marshal, with almost all deficiencies corrected timely.
- Additional duty safety officer/Building maintenance is quick to address building deficiencies.
- An annual test of the Emergency Operations Plan is conducted.
- Good general housekeeping.
- First aid supplies readily available.

Breckenridge Campus

- Additional duty safety officer participated in monthly safety meetings between West Texas campuses.
- Limited accidents occurring on campus.
- Periodic inspections by the State Office of Risk Management and the Fire Marshal, with almost all deficiencies corrected timely.
- City police and fire departments are readily available, with the fire department being just across the street.
- Additional duty safety officer/Building maintenance is quick to address building deficiencies.
- An annual test of the Emergency Operations Plan is conducted.
- Good general housekeeping.
- Welding gases properly stored.
- First aid supplies readily available.

Brownwood Campus

- Additional duty safety officer participated in monthly safety meetings between West Texas campuses.

- Quarterly building inspections are performed consistently.
- Limited accidents occurring on campus.
- Periodic inspections by the State Office of Risk Management and the Fire Marshal, with almost all deficiencies corrected timely.
- Monthly emergency light, AED, eyewash station and fire extinguisher inspections documented.
- Additional duty safety officer/Building maintenance is quick to address building deficiencies.
- An annual test of the Emergency Operations Plan is conducted.
- Good general housekeeping.
- Additional duty safety officer assists other West Texas campuses in performing electrical work/maintenance.

Ft. Bend County Campus

- Part-time Security Officer.
- Additional duty safety officer was trained by Harlingen's Safety Officer.
- Periodic inspections by the State Office of Risk Management and the Fire Marshal, with almost all deficiencies corrected timely.
- Cafe received an excellent grade on recent food handling inspection.
- MOU with Rosenberg Police Department to handle emergency calls.
- Recent purchase of first aid supplies for most labs/Student Services.
- Students in the Environmental Safety program assist the Additional duty safety officer conduct safety inspections and will assist in an upcoming tabletop exercise.
- Emergency telephones in elevators worked.

Harlingen Campus

- Full-time Police Department (10 commissioned officers and 3 other staff)
- Full-time safety officer on campus, with various buildings currently having designated additional duty safety officers.
- Safety officer and Police Department conduct various safety trainings.
- Lifts are inspected annually in Automotive.
- Welding gases properly stored.
- Periodic inspections by the State Office of Risk Management and the Fire Marshal, with almost all deficiencies corrected timely.
- Various safety trainings offered by Safety Officer and Police Department.
- An annual test of the Emergency Operations Plan is conducted.
- Cafeteria and Culinary Arts received excellent grades on recent food handling inspections.
- At least 1 artificial external defibrillator in every building.
- Eye wash/shower equipment are inspected weekly by instructors.
- Security cameras are in place and being monitored by TSTC Police Department.

- Good general housekeeping.
- In Housing:
    - Community Assistants perform bi-monthly safety inspections that include follow-ups on deficiencies, fines and evictions.
    - Community Assistants receive training from the Safety Officer.
    - Fire drills are performed each semester.

Marshall Campus

- Observations and deficiencies cited in past State Office of Risk Management and State Fire Marshal inspections were generally corrected quickly.
- Recent increase in maintenance personnel, who are responsive to facility issues.
- Fire extinguishers, artificial defibrillator devices, and first aid kits are inspected on a monthly basis.
- Contracts with a security company to provide armed security guards. These guards monitor security cameras located throughout campus, and perform hourly walk arounds. All guards were appropriately trained.
- Marshall Police and Fire Departments are readily available.
- Speed limit throughout campus is 10 MPH, with speed bumps placed in front of designated pedestrian road crossings.
- New first aid kits deployed throughout the campus.
- Welding gases properly stored.
- No large fuel tanks.
- Periodic inspections performed in housing, with security officer stationed in the housing area.

North Texas Campus

- Appointed a safety coordinator who receives an additional duty stipend for performing certain safety functions. The maintenance employee is active in this regard as well.
- Red Oak ISD Police Department and Red Oak Fire Department are readily available in case of emergencies.
- Facilities are being well-maintained.
- There are new first aid kits, and fire blankets available throughout the campus.
- There were not large fuel tanks present, and all chemicals were stored properly.
- Emergency phone in the only elevator worked.
- There were no deficiencies cited by the Fire Marshal in the most recent inspection.
- There were 4 artificial external defibrillator devices deployed in the building.
- Security cameras are in place and being monitored by the Red Oak ISD Police Department.
- General housekeeping was very good.

- All grinders had appropriate safety guards, and welding cylinders were properly stored.

Sweetwater Campus

- Additional duty safety officer conducted monthly safety meetings between West Texas campuses.
- Additional duty safety officer provides safety trainings for Building Maintenance and Custodial staff.
- Building Monitor and Storm Ranger Assignments and Emergency Response Notification Plan recently updated.
- Periodic inspections by the State Office of Risk Management, with almost all deficiencies corrected timely.
- Additional duty safety officer/Building maintenance is quick to address building deficiencies.
- An annual test of the Emergency Operations Plan is conducted.
- Creation of a State-wide Safety Meeting Attendance Sheet.
- Good general housekeeping.
- Full-time police department (5 commissioned officers).
- Cafeteria received an excellent grade on recent food handling inspection.
- In Housing:
    - Resident Assistants perform bi-monthly safety inspections with the Housing Director that include follow-ups on deficiencies, fines and evictions.
    - Safety violations receive a fine (no warnings).
    - Community Assistants receive training each semester.

Waco Campus

- Conducted a table top exercise within the last year of a realistic risk the campus faces.
- Maintains a full-time police department, with all officers attending required training.
- City of Waco maintains a full-time fire department on campus.
- Speed bumps in front of all pedestrian road crossings typically frequented by students.
- Full-time safety officer on campus, with each building currently having designated additional duty safety officers.
- Fuel tanks on campus (physical plant and airport) over 1,000 gallons have the appropriate spill containment measures, are appropriately registered, and document Spill Prevention, Control, and Countermeasure Plans in place.
- Emergency phones in all elevators worked.
- Vehicle lifts in the automotive instructional program are inspected on an annual basis.

- Welding gases are stored properly.
- In housing:
    - There are daily safety inspections in the family housing area that include follow-ups on deficiencies, fines and evictions.
    - Implemented and electronic database which allows for easier identification of recurring issues.
    - Employs its own inspectors and Residential Assistants in the dorms.
    - Implemented an aggressive plan for addressing past Fire Marshal issues that includes replacing old windows in family housing, ensuring smoke detectors are operational, replacing GFCI plugs and switches, and moving blocked breaker boxes.
    - Developed a rapport with the State Fire Marshal to demonstrate that past deficiencies are being aggressively addressed as resources permit.
- On the airport:
    - Vehicular access to airport runway is restricted to limited people and that require codes to the gates.
    - Control tower is fully staffed by 4 FAA certified controllers during weekdays, and 2 during weekends.
    - Frequent FAA inspections, with no findings.
    - Quarterly safety meetings.
    - Runways are checked for FOD on a daily basis.
    - Operations manual including safety procedures for airport
    - Airport is completely fenced, restricting vehicular and foot traffic.
    - All Fire Marshal deficiencies addressed.

Williamson County Campus

- Security guard on duty (employed by Temple College).
- Safety building inspections performed by Temple College.
- New facilities that are being well maintained.
- Periodic inspections by the Fire Marshal, with almost all deficiencies corrected timely.
- Annual inspection by the Hutto Fire Rescue.
- Annual test of the Emergency Operations Plan is conducted.
- Artificial external defibrillators are available throughout the building.

Summary of Finding

Improvements should be made to standardize safety processes between campuses, and to better establish College expectations and accountability.

Opinion

Based on the audit work performed, the College has implemented numerous safety and security controls to ensure students, employees and assets are reasonably safe. While we identified specific safety issues at each campus that need to be addressed, and there is a need to standardize processes across campuses, we found that the College generally provides a safe and secure environment. Management began addressing our observations and recommendations before this audit concluded to ensure safety remains a priority.

We would like to express our gratitude for the time and assistance provided by management and the staff at all campuses during this audit.

Submitted by:

Jason D. Mallory, CPA, CIA	June 11, 2018 Date

AUDIT FINDING DETAIL

Finding #1: Improvements should be made to standardize safety processes between campuses, and to better establish College expectations and accountability.

Criterion: During our audit, we tested 9 specific areas at each campus. Those included police/security presence, self-inspections, communication and handling of identified deficiencies, food handling, training, emergency alert system, fire controls, implementation of a comprehensive emergency operations plan, accident handling and reporting. We also performed on-site inspections at every campus. By performing the same procedures at each campus, we gained insight into whether key safety processes have been standardized, and identified common deficiencies that need to be corrected.

In addition to the specific safety deficiencies detailed in the confidential supplemental audit report, the following observations best illustrate the lack of standardized safety processes and understanding/accountability:

- The responsibility to maintain the first aid kits is unclear to employees. Consequently, the contents of kits we inspected varied from department to department, with many on some campuses being very old and inadequate.
- Accident reporting and handling is inconsistent. We found different versions of forms being used, with some documentation being unsigned and/or incomplete. And while there is a process for dealing with injuries requiring physician care, conversations with employees and a review of comments provided on some accident reports indicate the process is not well understood or effective at times.
- Accident trend analysis is, at best, informal. While we were able to piece together accident trends over the last 3 years using various reports, it appears that accident trends reported to the Board in the past have only included employee accidents related to worker's compensation claims. Numerous accidents (mostly minor) we identified during our testing involved students, and were not disclosed in executive management or Board reports. Trend analysis of all accidents would better focus training efforts and related resources.
- The frequency, reliability, and type of safety inspections and safety drills differ between campuses. Furthermore, documentation of those inspections were inconsistent.
- Safety related signage is outdated and inconsistent. And, there is not a College-wide standard for such signage. Similar to the first aid kits, there is not an understanding of whose responsibility it is to maintain signage.
- Accountability for safety deficiencies is not well defined. While a Safety Department that employs two full-time safety professionals exists, their efforts are primarily dedicated to the campuses they office at, with support being given to the other campuses. When they identify deficiencies warranting attention, the deficiencies are, at times, treated by line supervisors as suggestions. Consequently, those deficiencies are not corrected, and senior

levels of management are not always informed of risks that are being accepted, as there is not a formal reporting process.

- Responsibilities and roles are defined differently from campus to campus. As stated above, some campuses have full-time safety professionals, with buildings having designated safety representatives. Other campuses have safety coordinators who receive additional duty stipends to perform safety duties in addition to their official roles. As evidenced by recent fire marshal deficiencies and observations we made during this audit, deficiencies are not always identified and/or addressed expeditiously.
- Certain safety controls, such as artificial defibrillator devices (AEDs) and emergency phones, are deployed differently on each campus. For AEDs, some campuses have several in one building, while other campuses have them placed strategically in only select buildings. For emergency phones, one multi-building campus has several, while other multi-building campuses do not have any.
- Annual tabletop exercises of the emergency operations plan are not performed at every campus. Recent events within the last three years have demonstrated the College can mobilize quickly when required, but they also demonstrate the need to be prepared. Periodic exercises only assist with that preparation.

The creation of the Safety Department in 2015 indicates that the College has been moving towards standardization since its consolidation. The observations made in this audit indicate efforts are still required.

Consequences: By not specifically defining expectations and standardizing safety processes throughout the College, the definition of safety becomes subjective, as does the level of implementation and care. Achieving the goal of Placing More Texans depends on a safe and secure environment in which to operate and instruct.

Possible Solution: We recommend a standardized system of safety and security be implemented at each campus, and, at a minimum, consider the observations noted above and on the supplemental report. That system should include frequent inspections using defined criteria, and be evidenced by inspection reports that detail deficiencies and required corrective action plans. Follow-up inspections on any deficiencies should be integral to that process. The system should also include targeted training based upon formal analysis of various trends and risk profiles. Because the College already has a Safety Department in place, we recommend this Department oversee enhancements, validate the deficiencies cited in our audit, and be primarily responsible for the inspections and training going forward.

Management Response:

Division: Student Services/Safety Department
Executive Management: Rick Herrera, VC/CIO

Task	Brief Description	Responsible Individual	Completion Date
1.1	We are currently reviewing all safety processes, and will be standardizing them throughout the State. Our efforts will, at a minimum, address all observations noted in the audit report and include follow-up of the individual safety issues notes at each campus as detailed in the supplemental report. The revised processes will include a designated safety officer performing frequent inspections, along with training individual departments.	Susan Shafer, Enrique Carrillo	8/31/19

To: Donald Laforce, Director of Cybersecurity
Rick Collatos, Director of IT Infrastructure Operations
Shelli Scherwitz, Director of IT Support Operations

From: Jason D. Mallory, Audit Director
Subject: TAC 202 Compliance Follow-up Audit Report [18-003A]
Date: June 15, 2018

We recently completed a follow-up audit on the Texas Administrative Code 202 (TAC 202) Compliance Audit. The primary objective was to test controls we that were not implemented during the original audit dated June 28, 2017, and to test the 29 controls we were unable to test during that audit. The purpose of this memo is to disclose the controls that we found to be implemented vs. not.

RESULTS

TAC 202 Control Family	Implemented	Implemented with Recommendations	Not Implemented	Total Required Controls
Access Control	6	1	5	**12**
Authority and Purpose	0	0	0	**0**
Accounting, Audit, Risk Management	0	0	0	**0**
Awareness and Training	3	1	0	**4**
Audit and Accountability	3	4	3	**10**
Security Assessment and Authorization	3	2	2	**7**
Configuration Management	2	0	6	**8**
Contingency Planning	4	2	1	**7**
Data Quality and Integrity	0	0	0	**0**
Data Minimization and Retention	0	0	0	**0**
Identification and Authentication	5	0	2	**7**
Individual Participation and Redress	0	0	0	**0**
Incident Response	4	2	1	**7**
Maintenance	3	0	1	**4**

Media Protection	2	1	1	**4**
Physical and Environmental Protection	7	2	1	**10**
Planning	1	0	2	**3**
Program Management	10	5	1	**16**
Personnel Security	2	4	2	**8**
Risk Assessment	2	1	1	**4**
System and Services Acquisition	3	1	3	**7**
System and Communications Protection	4	1	6	**11**
Security	0	0	0	**0**
System and Information Integrity	2	1	3	**6**
Transparency	0	0	0	**0**
Use Limitation	0	0	0	**0**
Total	**66**	**28**	**41**	**135**
	48.89%	**20.74%**	**30.37%**	**100%**

Controls noted as Implemented were found to be operating according to all of the TAC 202 requirements. Controls notes as Implemented with Recommendations were found to substantially operate according to the requirements and controlled the intended risks, but there were minor opportunities to improve. Finally, the controls identified as Not Implemented were found to either not be implemented, or were not in a state that we can give assurance they are controlling the intended risks.

CONCLUSION

The majority of the information security controls defined by TAC 202 have been implemented. Management is currently continuing their efforts to implement the others. In FY 2019, we will again perform the biennial audit, with emphasis being placed on the controls that are not currently implemented. We will also test a sample of the ones we previously verified as implemented. We would like to express our gratitude for the time and assistance provided by all staff during this follow-up audit.

Submitted by:

June 15, 2018

Jason D. Mallory, CPA, CIA — Date

cc: Mike Reeser, Chancellor/CEO
Ricardo Herrera, VC/CTO
Audit Committee

To: Peggy Wilkey, Executive Director Purchasing
Linda Rodriguez-Guillen, Executive Director Purchasing
Gisela Figueroa, AVC Financial Services

From: Jason D. Mallory, Audit Director

Subject: Statewide Fixed Asset Control Follow Up Audit (18-037A)

Date: June 15, 2018

Departmental audits we performed in fiscal years 2017 and 2018 tested fixed assets and controlled items assigned to individual employees. These tests verified purchased and donated items meeting cost thresholds are being properly capitalized and recorded in the fixed asset system, and verified the custody and ongoing tracking of those items properly safeguard them from loss, theft, and misuse. In all of the audits we performed, we determined that qualifying purchased items are properly capitalized, and recorded in the fixed asset system. However, some audits revealed tracking and custody controls needed attention. As a result, we elected to perform a follow-up audit this fiscal year throughout the College to ensure fixed asset are properly safeguarded through implementation of prudent tracking and custody controls.

The purpose of this memo is to describe the results our follow-up audit, and explain why we do not feel procedures are yet at a point that allows us to remove the outstanding fixed asset item from our quarterly follow-up schedule.

RESULTS & RECOMMENDATIONS

We tested the following areas in this follow-up audit:

- The annual inventory process to ensure all asset custodians accurately accounted for their assets in FY 2017 by following the established procedures.
- Asset records to ensure they are updated by the inventory control technicians based upon notations documented by stewards on the annual inventory forms.
- Timely asset transfers, especially those assigned to employees who are no longer employed by the College.
- Disposal of assets to ensure those assets can be traced to legitimate disposal documentation.
- Donations to ensure a process for donations is being followed.

We also tested a limited sample of purchases to ensure assets meeting established thresholds are still being capitalized and recorded, and we traced samples of assets recorded on the fixed asset system to the actual assets that were on hand.

We determined that assets when purchased are properly recorded, assigned to an employee for safeguarding, and recorded in the fixed asset system. We were also able to verify assets recorded in the fixed asset system are on hand. Finally, the donation process seems to be generally working properly when assets are donated directly to the Foundation. In another project we performed concurrently with this one, we identified a department who had vehicles on hand that were reportedly donated directly to them (not the Foundation), but were not recorded in the College's records. Specific recommendations were issued to management in that department during that project, but we recommend as part of this audit that a communication be made to all employees during the fiscal year 2018 annual inventory process to report assets in their custody that are not already reflected on their inventory forms.

We identified processes that still require attention to ensure all assets are properly safeguarded after purchase. The following describes our findings and related recommendations.

- For the 2017 annual inventory process, documentation was missing for some stewards which evidenced that their assets were inventoried. We also identified instances where changes/updates were notated by some stewards on their inventory forms, but asset records were not updated to reflect those changes. We recommend that inventory control technicians reconcile all stewards who need to perform an annual inventory to documentation that is actually received, and escalate the matter to appropriate management when reasonable follow-up requests with the employees do not work. We also recommend the inventory control technicians more closely monitor inventory forms being submitted, and update the fixed asset system to reflect all notations made by stewards.
- We identified some assets that were transferred from one steward to another without appropriate documentation being on file to indicate the receiving steward accepted responsibility for the asset. We recommend that all transfers be supported by documentation signed by both the person releasing the asset and the person receiving it.
- We identified some assets currently assigned to people who are no longer employed by the College. The assets should have been transferred to an active employee for safekeeping. In one case numerous assets were not transferred for several months after the person left employment. Once the transfer process began, the assets could not be located. Those assets had a combined estimated value of $103,000. We recommend that all assets be transferred to active employees during the campus clearing process to ensure accountability for missing items is assigned to the appropriate steward. This is especially important when the separation is not voluntary.
- For some assets coded as disposed, we were unable to determine where the assets actually went. And, based upon a review of records and observation of an asset in the warehouse, we determined that assets scheduled for disposal are sometimes coded as disposed prior to them actually being sold and removed. We recommend better records be maintained so that all assets coded as disposed can be traced to their final disposition. We also recommend that assets not be marked as disposed until ownership has been actually transferred.

CONCLUSION

We recognize the recent efforts directed towards asset control, and commend management for those efforts. We feel addressing the issues cited above will ensure all assets are reasonably safeguarded, and improve accountability in that regard. In our opinion, these outstanding issues warrant further testing after the fiscal year 2018 annual inventory process is complete. We will perform that testing in fiscal year 2019. We would like to express our gratitude for the time and assistance provided by all staff during this follow-up audit.

Submitted by:

Jason D. Mallory, CPA, CIA	June 15, 2018 Date

MANAGEMENT RESPONSE

All inventory asset control staff and directors had a training session with accounting and reporting staff where the team identified ways to ensure the inventory sheets are collected in full in the future. Management will going forward reconcile all stewards who need to complete annual inventory documentation to documentation that is actually received, and escalate the matter to appropriate management when reasonable follow-up requests with the employees do not work and/or proper documentation in the event of a form being turned in late or missing. (16 out of 238 in FY17 and 2 out of 238 in FY18). We will also more closely monitor inventory forms being submitted, and update the fixed asset system to reflect all notations made by stewards. During our last audit we decided that we were going to transfer assets of employees leaving the college to the supervisor even when not signed within 2 weeks. While this seemed like a good business practice in theory, the reality was that we ended up with unsigned sheets. After reviewing that practice we decided to go back to getting signatures before transfer. Management well ensure that all transfers are supported by documentation signed by both the person releasing the asset and the person receiving it or in the case of employee separation, have the receiving steward acknowledge receiving the assets.Procurement will work together with Human Recourses to ensure that all assets are transferred to active employees during the campus clearing process to ensure accountability for missing items is assigned to the appropriate steward. Management understands that this is of key importance specially when the separation is not voluntary. Management will work to maintain better records so that all assets coded as disposed can be traced to their final disposition. Management will also ensure that assets not be marked as disposed until ownership has been actually transferred.

cc: Mike Reeser, Chancellor/CEO
Jonathan Hoekstra, VC/CFO
Audit Committee

TEXAS HIGHER EDUCATION
COORDINATING BOARD
P.0. Box 12788 Austin, Te_ms 78711

512/427-6101
Fax 5121427-6127

Website:
http://www.thecb.state.tx.us

May 9, 2018

Mr. Michael Reeser, Chancellor
Texas State Technical College - Waco
3801Campus Drive
Waco, TX 76705

Dear Mr. Reeser,

I am attaching the final report on *A Compliance Desk Review of Texas Educational Opportunity Grant at Texas State Technical College - Waco,* Report No. THECB-CM- FA-18-025. There were no findings resulting from this engagement.

Texas State Technical College - Waco (TSTC) complied with relevant Coordinating Board (THECB) rules and regulations for the Texas Educational Opportunity Grant (TEOG) and with the Texas Administrative Code (TAC) §22.253 through 22.263.

Summary

Our desk review included tests of relevant financial data reported and certified by TSTC for award year 2016-2017. We believe the evidence obtained provides a reasonable basis for the findings and recommendations, if any, based on the desk review objectives.

Our work included procedures to verify:

- Students met all eligibility criteria, including SAP requirements;
- Students demonstrated financial need;
- Students fulfilled residency requirements;
- Applicable students registered with the selective service system; and
- Reported award amounts reconciled with Texas State Technical College's student data system and payment records.

The cooperation of your staff during this review is greatly appreciated. If you have any questions or comments on the conduct of this engagement, please let me know.

Sincerely,

Mark A. Poehl

Mark A. Poehl, CPA, CIA, CISA, CFE
Director, Internal Audit and Compliance

PERFORMED BY:
Ms. Jamyen Robinson-Hall, Compliance Specialist

cc:

THECB
Board Members

Commissioner's Office
Dr. Raymund A. Paredes, Commissioner of Higher Education
Ms. Linda Battles, Deputy Commissioner for Agency Operations and Communication/COO
Dr. David Gardner, Deputy Commissioner for Academic Planning and Policy
Mr. William Franz, General Counsel
Mr. Ken Martin, Assistant Commissioner of Financial Services & Chief Financial Officer

Student Financial Aid Programs
Dr. Charles Puis, Deputy Assistant Commissioner, Student Financial Aid Programs

Texas State Technical College
Mr. John K. Hatchel, Chairman/ Board of Regents
Mr. Adam Hutchison, Provost
Mr. Rick Herrera, Vice Chancellor
Ms. Christine Stuart-Carruthers, Division Manager
Ms. Jackie Adler, Executive Director of Financial Aid
Mr. Jason Mallory, Director of Internal Audit

STATUTORY DISTRIBUTION REQUIREMENT
State Auditor's Office
Internal Audit Coordinator
Sunset Advisory Commission
Mr. Ken Levine, Director

State Auditor's Office

March 30, 2018

Mr. Jason Mallory, Director of Audits
Texas State Technical College System
3801 Campus Drive
Waco, TX 76705

Re: Audit Delegation Request 719-2018-001

Dear Mr. Mallory:

In accordance with Texas Government Code, Section 321.020, and subject to the conditions listed in Attachment A, the State Auditor's Office delegates to the Texas State Technical College System (System) the authority to employ a private auditor to conduct an audit of the System's financial statements for fiscal year 2018 and federal compliance as required by the Southern Association of Colleges and Schools Commission on Colleges (SACSCOC) during the re-accreditation process, as described in your online request.

If you have any questions, please contact James Timberlake, Audit Manager, or me at (512) 936-9500.

Sincerely,

Verma L. Elliott, CPA, CIA, CGAP, MBA
Assistant State Auditor

Attachment

Robert E. Johnson Building
1501 N. Congress Avenue
Austin, Texas 78701

P.O. Box 12067
Austin, Texas 78711-2067

Phone:
(512) 936-9500

Fax:
(512) 936-9400

Internet:
www.sao.texas.gov

Attachment A

This delegation of authority is subject to the following:

1. The System will provide the State Auditor's Office with advance notice of key meetings in a timely manner. Examples of key meetings include entrance and exit conferences, meetings regarding internal control assessments, and status meetings. State Auditor's Office representatives may attend key meetings related to any audit engagement the System enters into under this delegation of authority.

2. The System will notify the State Auditor's Office if an amendment to the contract significantly alters any contract terms, including, but not limited to, the scope of work to be performed and the term of the contract.

3. The System will comply with applicable law, policies, and procedures in the procurement of audit services, the expenditure of funds under the contract, and all other aspects of forming and administering the contract with the private auditor.

4. The System will ensure that the State Auditor's Office promptly receives a copy of any report resulting from a peer review of the private auditor that is received by the private auditor after entering into the contract with the System.

5. Any contracts entered into under this delegation of authority will include the following language:

   a) The Contractor understands that acceptance of state funds under this contract acts as acceptance of the authority of the State Auditor's Office to conduct an audit or investigation in connection with those funds. The Contractor further agrees to cooperate fully with the State Auditor's Office in the conduct of the audit or investigation, including providing all records requested. The Contractor will ensure that this clause concerning the State Auditor's Office's authority to audit state funds and the requirement to cooperate fully with the State Auditor's Office is included in any subcontracts it awards. Additionally, the State Auditor's Office shall at any time have access to and the rights to examine, audit, excerpt, and transcribe any pertinent books, documents, audit documentation, and records of the Contractor relating to this contract for any purpose.

   b) The Contractor understands that the State Auditor's Office may opt to rely on the work of the Contractor to support the State Auditor's Office's opinion on the Comprehensive Annual Financial Report for the State of Texas, and the Contractor agrees to cooperate with the State Auditor's Office in a joint effort to comply with American Institute of Certified Public Accountants standard AU-C 600, *Special Considerations-Audits of Group Financial Statements {Including the Work of Component Auditors).* The Contractor agrees that the State Auditor's Office is serving in the capacity of the group engagement auditor. As a component auditor, the Contractor agrees to provide to the State Auditor's Office information necessary to facilitate determinations regarding the Contractor's understanding and compliance with ethical requirements and professional competence.

6. If the State Auditor's Office determines that it cannot rely on the Contractor's work to support the State Auditor's *Office's* opinion on the Comprehensive Annual Financial Report for the State of Texas for any reason, including a lack of cooperation in complying with AU-C *600,* it may be necessary for the State Auditor's Office to perform additional work at the System and to be reimbursed by the System in accordance with Article X of the *State's* General Appropriations Act and the Interagency Cooperation Act (Texas Government Code, Chapter 771). Related questions may be directed to Michael Clayton, Audit Manager, at (512) 936-9500.

7. If the terms of the agreement with the private auditor are set forth only in an engagement letter, the engagement letter will include the language quoted in #5 above.

8. A signed copy of the contract or contract amendment should be provided to the State Auditor's Office within two weeks of execution. For risk assessment purposes, the State Auditor's Office should have access to any draft audit reports and should be provided a copy of such reports upon request. Additionally, the System will provide the State Auditor's Office with copies of all final audit reports and other deliverables provided under the contract-including reports on internal controls and compliance, management letters, or reports to management-within two weeks of completion. You may submit the contract and audit reports electronically to auditdelegation@sao.texas.gov or submit hard copies to the attention of Audit Delegation. Please include the audit delegation request number 719-2018-001 with all submissions and related correspondence.

9. The System will promptly notify the State Auditor's Office if any deliverable that is subject to a financial reporting deadline established by the Comptroller of Public Accounts will not be completed by that deadline.

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 issues were reported this quarter.			

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.