

**Texas State Technical College  
Board of Regents  
Audit Committee Meeting  
3801 Campus Drive  
Col. James T. Connally Aerospace Center  
Board Room  
Waco, TX**

**Thursday, August 12, 2015  
10:45 a.m.**

**AGENDA**

- I. Meeting Called to Order by Audit Committee Chair Joe Gurecky**  
[Joe Gurecky, Joe Hearne, Keith Honey]
- II. Committee Chair Comments**
- III. Minute Order:**  
**Proposed MO #**
- [31-15\(c\) Proposed Audit Plan for Fiscal Year 2016](#) .....2
- IV. Reports:**
- [Status of Fiscal Year 2015 Audit Schedule & Other Projects](#) .....8
- [Summary of Audit Reports](#) .....10
- [Follow-up Schedule and Status](#) .....13
- [Breckenridge: Safety & Security Audit](#) .....18
- [Brownwood: Safety & Security Audit](#) .....23
- [Harlingen and Waco: VA Benefits Compliance Audit](#) .....28
- [Internal Audit: External Quality Assessment Review](#) .....34
- [Marshall: Safety & Security Audit](#) .....47
- [North Texas: Safety & Security Audit](#) .....53
- [OIT: External Network Penetration Test](#) .....59
- [AY 2014 A-133 Evaluation & Desk Review Management Letter](#) .....66
- [Attestation Disclosures](#) .....67
- 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 previous 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 13, 2015

**Proposed Minute Order #:** 31-15(c)

**Proposed By:** Jason D. Mallory, Director of Audits

**Subject:** Proposed Audit Plan for Fiscal Year 2016

**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 2016.

**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 2016

**Recommended Minute Order:** “The Board of Regents approves the audit plan for fiscal year 2016.”

**Recommended By:**



---

Jason D. Mallory, Director of Audits



**Internal Audit Department**

## **Audit Plan**

**Fiscal Year 2016**

**Proposed August 13, 2015**

## Executive Summary

### Table of Contents

Executive Summary .....	1
Description of Risk-Based Methodology .....	1-2
Description of Project Types .....	2
Proposed Audit Plan .....	2-4

The purpose of the Audit Plan (Plan) is to outline audits and other activities the Internal Audit Department will conduct during fiscal year 2016. The Plan was developed to satisfy Internal Audit responsibilities established by the Internal Audit Charter (SOS GA.1.4), the Texas Internal

Auditing Act (Section 2102.008), and other audit standards.

The Plan was established using available risk information at the time, therefore, 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 Audit Committee and Executive Management of requested revisions to the Plan.

A comprehensive risk-based methodology was used in establishing the Plan. The process considered high-level risks to numerous processes within the Colleges. Input from Executive Management and the Audit Committee was an integral part of the methodology.

The Plan includes 9 audits, at least 8 follow-up audits, and 3 scheduled other projects. Additionally we will perform investigations and other audit work through-out the year as those opportunities arise.

## Description of Risk-Based Methodology

A comprehensive risk-based methodology was used in developing the Plan. That methodology included ranking potential audits using the ten risks listed below:

1. Asset Liquidity/Fraud
2. Regulatory Compliance
3. Quality of Internal Control
4. Financial Statement Impact
5. Importance and Integrity of Data and Reports
6. Management/Board Interest
7. Frequency, Complexity, and Volume of Transactions
8. Changes in Systems, Processes, or Procedures
9. Results and Time Since Last Audit
10. Customer Impact

Once all potential audits were ranked, a list of audit candidates (the Plan) was developed based upon the risk rankings.

The list of potential audits that were risk ranked are stored in a database that was created by reviewing past audit work, flowcharts, organizational charts, and general industry processes. Input from management and the audit staff was also used in developing the database. It is updated frequently to reflect recently completed audits, and new auditable activities.

The Plan is considered in light of significant activities occurring at the College and in the industry. Some of those activities this year included single accreditation efforts, performance based funding, increased marketing efforts, and actions aimed at building a culture of

philanthropy. Other's included management's stated intent to maximize alternative funding sources such as grants and auxiliary business profits, specific actions aimed at operating more efficiently in administrative functions, increased IT security efforts, and legislative requests. The most recent year-end financial statements, industry related news and events, recent legislation, and past audit plans from other colleges (particularly those in Texas) were also considered.

The Plan is considered a proposal, and subject to revision if circumstances change.

### **Description of Project Types**

Audits: These are projects in which some activity or other management assertion is evaluated so that an opinion can be offered. These can also be projects in which the object is not to offer an opinion, but to develop new information on an activity so that management can use that information in their decision making process.

Follow-up Audits: These are projects in which deficiencies identified in a past audit are tested to ensure management applied appropriate corrective action.

Other Projects: These include fraud investigations, special projects requested by the Board or management, assistance given to external auditors, and administrative projects within the department.

### **Proposed Audit Plan**

#### **External Audits**

A-133 Follow-up Audit of Federal Awards (Harlingen): The State Auditor's Office will test financial aid deficiencies identified in FY 2014 to ensure those have been corrected. Limited assistance will be offered by Internal Audit.

A-133 Follow-up Audit of Federal Awards (Marshall): The State Auditor's Office will test financial aid deficiencies identified in FY 2014 to ensure those have been corrected. Limited assistance will be offered by Internal Audit.

A-133 Follow-up Audit of Federal Awards (Waco): The State Auditor's Office will test financial aid deficiencies identified in FY 2014 to ensure those have been corrected. Limited assistance will be offered by Internal Audit.

A-133 Follow-up Audit of Federal Awards (West Texas): The State Auditor's Office will test financial aid deficiencies identified in FY 2014 to ensure those have been corrected. Limited assistance will be offered by Internal Audit.

Internal Network Penetration Test (Office of Information Technology): An external consultant (TBD) will test internal threats to the security of the College's IT network.

#### **Internal Audits, Follow-up Audits & Other Projects**

Public Funds Investment Act Audit (Accounting & Finance): This audit is required by the Public Funds Investment Act to be performed every two years. Policies, investment strategies, training, reporting, and calculations will be tested in this audit.

---

Benefits Proportionality Audit (Accounting & Finance, Human Resources): In FY 2014, all State agencies were requested by the Governor's Office to audit benefits proportionality to ensure employee benefits were paid in proportion to the fund the fund(s) that paid the salaries. Once again, agencies are being asked to audit this activity. It is anticipated the State Auditor's Office will standardize audit procedures and scope.

Violence Against Women Act (VAWA) & Campus Sexual Violence Elimination Act Compliance Audit (Operations Division): Sexual assaults and dating violence on campuses are a serious concern at institutions of higher education. To help reverse that trend, sweeping new mandates and government recommendations were handed down in the VAWA and Campus SaVE Act. The new legislation, which goes into full effect on July 1, 2015, not only requires better monitoring, reporting, and incident management from schools, but also educational initiatives. This audit will test compliance to these regulations.

College Assistance Migrant Program (CAMP) Grant (Operations Division - Harlingen): With an award amount of over \$2 million awarded by the US Department of Education, this audit will test compliance to the grant provisions, to include meeting the grant objectives, properly accounting for the funds, and reporting information timely.

Developmental Education Scaling and Sustaining Success Grant (Operations Division– West Texas): With an award amount of over \$320 thousand awarded by the Texas Higher Education Coordinating Board, this audit will test compliance to the grant provisions, to include meeting the grant objectives, properly accounting for the funds, and reporting information timely.

Portal Application Audit (Office of Information Technology): The Portal is a web-based application that allows the College to disseminate information to employees. It is also increasingly being used as a gateway to other College systems, such as Colleague. This audit will test select application controls that ensure the Portal is secure and functions properly.

Discretionary Purchases Audit (all College Divisions): Annually, tens of millions of dollars are spent on purchases. This audit will identify and scrutinize current year and prior year spending that may be unnecessary to fulfill the College's core business of education.

Student Worker's Audit (all College Divisions): This audit will determine the necessity for student workers, verify the appropriate use of them, and ensure controls around them are adequate.

2015 Safety & Security Audits - Follow-up Audits: We will test deficiencies identified in the 2015 safety audits to ensure management applied the appropriate corrective actions.

2014 Employee Time Reporting Audit – Follow-up Audit: We will test deficiencies identified in the 2014 audit to ensure management applied the appropriate corrective action to ensure that reported employee time is correct. The original audit stemmed from a fraud investigation in which an employee reported and was paid for time that he obviously did not work.

2015 West Texas Skills Development Grant Audit – Follow-up Audit: We will test deficiencies identified in the 2015 audit to ensure management applied the appropriate corrective actions to ensure the grant deliverables are met, and that reporting is correct and timely.

2016 Audits – Follow-up Audits: If any deficiencies are identified in the FY 2016 audits, we will perform follow-up testing as needed.

FY 2015 Annual Audit Report: An Annual Report will be prepared in accordance to the Texas Internal Auditing Act. This report will summarize the audit activities over the past fiscal year.

External Quality Assessment Review at SFA University: To participate in the peer review program that produced our 2015 Internal Audit External Quality Assessment Review, we must reciprocate by providing similar services at another institution. All expenses are paid by SFA. The benefits of participating in this program include low costs associated with our periodic peer review, and staff development.

Facilitate Quarterly Attestation Process: Internal Audit will continue to facilitate the attestation process to ensure all reports are made on a timely basis.



**Texas State Technical College  
Internal Audit  
Status of Fiscal Year 2015 Audit Schedule & Other Projects**

Description	Location	Status	Report No.	Report Date
<b>INTERNAL AUDITS</b>				
Disaster Recovery Test - Colleague	OIT	Complete	15-015A	9/10/2014
Safety & Security Audit	Waco	Complete	15-012A	12/4/2014
Skills Development Grant Audit	West Texas	Complete	15-006A	12/9/2014
Surprise Police Evidence Inspection	Waco	Complete	15-024A	12/10/2014
Safety & Security Audit	Harlingen	Complete	15-013A	12/12/2014
Safety & Security Audit	Ingelside	Complete	15-022A	12/18/2014
Purchasing Fraud Audit	Statewide	Complete	15-019A	1/9/2015
Skills Development Grant Audit	Marshall	Complete	15-021A	3/9/2015
Quarterly External Port Scan	OIT	Complete	15-016A	3/11/2015
Safety & Security Audit	Abilene	Complete	15-028A	3/17/2015
Safety & Security Audit	Sweetwater	Complete	15-026A	3/17/2015
Safety & Security Audit	EWCHEC (Hutto)	Complete	15-032A	3/18/2015
Safety & Security Audit	Ft. Bend	Complete	15-027A	3/18/2015
Safety & Security Audit	Breckenridge	Complete	15-038A	5/22/2015
Safety & Security Audit	Brownwood	Complete	15-037A	5/22/2015
Safety & Security Audit	Marshall	Complete	15-033A	6/15/2015
Safety & Security Audit	North Texas	Complete	15-035A	6/16/2015
VA Benefits Audit	Harlingen	Complete	15-029A	6/23/2015
VA Benefits Audit	Waco	Complete	15-030A	6/23/2015
IT Security Follow-up Review	OIT	In Progress		
VA Benefits Audit	Marshall	In Progress		
VA Benefits Audit	West Texas	In Progress		
<b>EXTERNAL AUDITS</b>				
Texas Department of Public Safety: On-site Audit	Waco	Complete		5/22/2014
THECB: AY 2013 A-133 Evaluation and Desk Review	West Texas	Complete		9/25/2014
State Auditor's Office: A-133 Follow-up	Harlingen	Complete		2/27/2014
State Auditor's Office: A-133 Follow-up	Waco	Complete		2/27/2014
State Auditor's Office: A-133 Follow-up	West Texas	Complete		2/27/2014
State Auditor's Office: A-133 Testing for Statewide Single Audit (Financial Aid)	Marshall	Complete		2/27/2014
State Comptroller's Office: Post-Payment Audit	Statewide	Complete		1/8/2015
Patillo, Brown & Hill: FY 2013 & 2014 Review of Consolidated Financial Statements	Statewide	Complete		3/4/2015
MainNerve: External Network Penetration Test	OIT	Complete		6/17/2015



<b>Description</b>	<b>Location</b>	<b>Status</b>	<b>Report No.</b>	<b>Report Date</b>
Groover & Charbonneau: External Quality Assessment	Internal Audit	Complete	15-020A	4/29/2015
Texas Workforce Commission: Wagner Peyser Grant #1315WPB000	Office of Sponsored Programs	In Progress		

#### **OTHER INTERNAL PROJECTS**

SAO Hotline: Allegation - State and Federal financial aid was awarded fraudulently. Results - Did not find any violations of State or Federal rules.	Harlingen	Complete	15-014I	10/7/2014
Internal review of an employee's purchases to ensure they are all legitimate. Requested by management. Results - Did not identify any fraudulent purchases, and determined that management's system of internal controls was sufficient to identify attempts.	Harlingen	Complete	15-025I	1/27/2015
SAO Hotline: Allegation - College resources were misappropriated for personal use. Results - Determined that the allegation had no merit.	Waco	Complete	15-034I	3/26/2015
THECB: Allegation - Supervisor allowed subordinates to take vacation time without charging it. Results: HR reviewed this allegation and determined that the supervisor was inappropriately allowing overtime to be "banked" and used in lieu of vacation. The practice was	Waco	Complete	15-039A	6/1/2015
Internal report that an employee has inappropriately benefited from a TSTC contract.		In progress		
Internal report that an employee was not paid for all work he/she performed.		In progress		



**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
<b>Breckenridge: Safety &amp; Security Audit (15-038A)</b>	No reportable exceptions noted. Specific recommendations were made to management to enhance safety procedures.				
<b>Brownwood: Safety &amp; Security Audit (15-037A)</b>	No reportable exceptions noted. Specific recommendations were made to management to enhance safety procedures.				
<b>Harlingen &amp; Waco: VA Benefits Compliance Audit (15-029A &amp; 30A)</b>	1. A centralized and standardized method for maintaining and monitoring documentation, and reporting enrollment data to the VA needs to be implemented. The processes currently on both campuses varies, with documentation and reporting exceptions noted at both.	Record keeping methods varied not only within the same office on the same campus, but also between campus offices. Since January 2015, management has been actively involved in identifying and resolving such difference. There were instances where we did not find required documentation in the VA files nor in files of other College departments. We also found instances where courses were taken that were not part of the approved program of study for the student, and instances where enrollment certifications and changes were not timely reported.	1.1 We will: - Centralize files that contain all required documents for every student by scanning all documents for safekeeping in ImageNow. - Because some offices do not have scanners, equipment will need to be purchased as resources permit. - All school certifying officials will begin using curriculum information obtained from the THECB to evaluate courses and programs of study. - Obtain access to required documents maintained by other departments and determine a way to organize these. We feel these steps will help us better meet monitoring and reporting requirements.	Adams	Immediately
<b>Internal Audit: External Quality Assessment Review (15-020A)</b>	1. Working papers prepared by the Director of Audits are generally not reviewed by another member of the department prior to issuance of the audit report.		1.1 The working papers prepared by the Director will be reviewed by another person in the Department.	Mallory	Immediately
	2. Internal quality control procedures have not been reported annually to the Audit Committee.		1.2 An annual report to the Board will be prepared that lists the quality control procedures that are in place over the internal audit process.	Mallory	8/13/2015
	3. Current procedures for continuing professional education do not require each auditor to obtain at least 40 hours per year. The internal policy requires 40 hours to be obtained by auditors in a 2-year period.		1.3 I did not realize the different standards conflicted on this requirement. In practice everyone in the Department has obtained close to 40 hours or more of education annually, however our departmental policy only requires 20 hours. That policy will be updated to require at least 40 hours annually rather than 20.	Mallory	Immediately
	4. Ongoing monitoring of the performance of the internal audit activity is being conducted; however, periodic self-assessments should be completed more frequently to enhance compliance with the Standards.		1.4 The standards only require periodic self-assessments, which we perform. The term "periodic" is not defined. But to further demonstrate our commitment to quality, we will begin performing and documenting a self-assessment every 1.5 years, and reporting the results to the Board.	Mallory	Immediately

Report Name & No.	Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
	5. An audit of TSTC's ethics and IT governance programs should be conducted periodically to enhance compliance.		1.5 The ethics and IT governance audit recommendation implies that performing specific audits every 3 years is a requirement. But in fact compliance guidance included in the actual standards clearly state that we must be familiar with these processes, and that an understanding is most likely obtained through several different audits and processes. We will include these individual audits in our annual audit planning process, and perform them only if <u>the risk rating is high in comparison to other auditable</u>	Mallory	Immediately
	6. The TSTCIAD should increase audit coverage to ensure periodic audits of major systems such as Colleague, learning management systems, and the required audit of Texas Administrative Code 202 (required every two years) are conducted.		1.6 In the past, specific IT audits similar to those listed in the peer review team's recommendation were performed because a dedicated IT auditor was on staff. After losing that resource, we have gradually been rebuilding that capacity through training and outsourcing, and will continue down that path. In 2015, four specific IT audits were scheduled which demonstrates our commitment to performing IT audits. Going forward, IT specific audit will continue to be included in the annual audit plan.	Mallory	Immediately
<b>Marshall: Safety &amp; Security Audit (15-033A)</b>	1. We identified one area we feel warrants management's consideration.	The details are included in a confidential supplemental report available upon request.	The details are included in a confidential supplemental report available upon request. All corrective actions are appropriate.	Day	8/31/2015
<b>North Texas: Safety &amp; Security Audit (15-035A)</b>	1. We identified one area we feel warrants management's consideration.	The details are included in a confidential supplemental report available upon request.	The details are included in a confidential supplemental report available upon request. All corrective actions are appropriate.	Rowland	8/31/2015
<b>OIT: External Network Penetration Test (15-043A) performed by MainNerve</b>	1. A TSTC web site was vulnerable to a SQL injection attack. MainNerve executed the SQL injection and subsequently retrieved student registration data, including full names, home addresses, email addresses, and telephone numbers. Other data of interest included TSTC staff-related information that contained contact information and work roles.		The site www.waco.tstc.edu was found to be vulnerable to SQL injection. The code that allowed this was immediately isolated and removed. Our Information Security personnel validated the correction by attempting to repeat the injection without success. Additionally, on July 1st 2015 the Waco.tstc.edu site will be deactivated in favor of the single tstc.edu website. We consider this item resolved, however, MainNerve will verify our assertion in follow-up testing.	Herrera	Immediately
	2. There are many systems exposed to the Internet with services that could be accessed and enumerated easily using clear text protocols, such as SNMP. By exploiting this misconfiguration, MainNerve downloaded specific details regarding the target system. Most of the systems detected were printers whose value lay in the fact that the internal IP address was disclosed. This information allows an attacker to profile the internal network for potential future attacks. MainNerve also connected to several printers sent print commands.		The ability to access select printers via the internet has never been an intended practice. We have eliminated the ability to access through the internet the specific printers identified by MainNerve. We are currently unaware of any printers with the same vulnerability, but will immediately eliminate the risks if they present themselves in the future. We consider this item resolved, however, MainNerve will verify our assertion in follow-up testing.	Herrera	Immediately

Report Name & No.		Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
	3.	Various Polycom telecom systems were detected with some being video enabled. Unauthenticated telnet sessions was permitted on one system wherein remote dialing over POTS (Plain Old Telephone System) call to a MainNerve facility was possible.		MainNerve was able to utilize default vendor credentials to access a video conferencing device, and were able to make phone calls from the device. We will remove the default credentials. This will also be verified in the upcoming MainNerve follow-up testing.	Herrera	Immediately
	4.	A host containing a critical vulnerability related to MS14-066 which could allow remote code execution by a remote user. MainNerve attempted to exploit this vulnerability on several occasions without success.		MainNerve detected and successfully exploited the Heartbleed vulnerability on a video conference type device in Harlingen. We updated the software which allowed this vulnerability, and will continue to work with all vendors to ensure software/firmware is always up to date. We consider this item resolved, however, MainNerve will verify our assertion in follow-up testing.	Herrera	Immediately
	5.	A system containing critical vulnerabilities related to the Novell eDirectory software was detected on a different TSTC web site.		Four SMTP servers discovered by MainNerve send emails from limited internal devices and applications. Even though SMTP servers are publicly visible, and our security safeguards were able to restrict MainNerve from doing anything. We consider this issue properly controlled.	Herrera	Immediately
AY 2014 A-133 Evaluation and Desk Review performed by THECB	1.	No exceptions 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
<b>December 2010 Attestation Disclosure, Herrera</b>	1.	TSTC provides internet service to members of the West Texas Telecommunications Consortium (WTTTC). In 2008, WTTTC was cited for an FCC violation in an external audit because the audit concluded that WTTTC "surrendered control of its competitive bidding process" to TSTC because a TSTC employee sat on the WTTTC board at the time. However, the audit went on to conclude that the selection of TSTC was the most cost effective bid. Nevertheless, as a result of this audit finding, the funding agency has indicated in letters to both TSTC and WTTTC that \$589 thousand may be required to be repaid. The certainty of that requirement is yet unknown.	TSTC and WTTTC issued an attorney drafted joint appeal on January 11, 2011, to the funding agency in an attempt to 1) clarify the audit finding, and 2) appeal the ruling that the money may need to be repaid. This appeal is based primarily on the facts that no negative monetary effect was felt by WTTTC, and the TSTC employee who was on the Board did not actually participate in any part of the bid process. The appeal also included affidavits from 4 WTTTC Board members, the WTTTC WAN Director, and the TSTC employee that state the TSTC employee did not participate in the bidding or selection process.	<b>On-going:</b> As of 11/25/14, we had not received a response on our appeal to the finding from the FCC. TSTC General Counsel spoke with our outside counsel on the matter and outside counsel indicated that the FCC is severely backlogged on appeals. They are just now reviewing appeals filed in 2006. Internal Audit will leave this on the follow-up schedule until the appeal has been heard. This may take several years.	We are still pending a ruling from the FCC on the matter.	Still awaiting FCC response
<b>Harlingen, Waco, Marshall, WT, Sys Ops: Employee Time Reporting Audit, Lawrence</b>	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.	<b>On-going:</b> On 06/19/14, Hannah Love indicated that they are working on a process where 2 people will be trained to scrutinize all ALPs, and better restricting access. She further stated that automation will continue to be explored.	Management has designated two employees within Human Resources to review all documentation provided by employees related to compensatory time. By September 2015 the campus locations will have fully transitioned from campus tracking to centralized monitoring of this process. By October 1, 2015 Human Resources will have completed the review of enhancements that would increase automation of this process. A year end adjustment to compensatory time will again be made in the appropriate system at the conclusion of this fiscal year.	10/1/2015
			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.	<b>See above comments</b>	Due to other critical projects related to single accreditation the review of additional automation options has not been completed. By October 1, 2015 Human Resources will have completed the review of enhancements that would increase automation of this process.	10/1/2015
			1.4 Once the method for time reporting is determined, System-wide training will be implemented.	<b>See above comments</b>	The two employees assigned to monitor this issue within Human Resources will receive additional training on this issue during the summer of 2015. Supervisors and related personnel will receive additional training after the review of automation options is completed.	10/1/2015

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
<b>Harlingen: A-133 Audit (performed by the SAO), Pena, Adams, Martin, Herrera</b>	1.	Summary: Cost of Attendance budgets need to be adjusted to reflect actual enrollment so that the potential for over awards is reduced.	Continue to calculate initial award on full-time enrollment, and after the census date adjust the cost of attendance to the actual enrollment level. Awards will continue to be adjusted as necessary.	<b>06/08/15:</b> SAO has begun follow-up testing. Those results will not be final until February 2016.		2/1/2016
	2.	Summary: The College did not maintain adequate access controls over financial aid functions in Colleague.	A. Revoke access. B. Reduce administrator rights to only 3 individuals. C. Remove the ability for programmers to migrate code to the production environment. D. Require mandatory account reviews, and sample accounts to ensure access is appropriate.	<b>06/08/15:</b> SAO has begun follow-up testing. Those results will not be final until February 2016.		2/1/2016
<b>Waco: A-133 Audit (performed by the SAO), Adler, Adams, Martin, Herrera</b>	1.	Summary: The College did not maintain adequate access controls over financial aid functions in Colleague.	A. Revoke access. B. Reduce administrator rights to only 3 individuals. C. Remove the ability for programmers to migrate code to the production environment. D. Require mandatory account reviews, and sample accounts to ensure access is appropriate.	<b>06/08/15:</b> SAO has begun follow-up testing. Those results will not be final until February 2016.		2/1/2016
	2.	Summary: All information that is required to be verified was not always done so accurately.	Verification was outsourced to EdFinancial in April 2013. College staff will periodically verify a random sample. Additionally a management report has been created.	<b>06/08/15:</b> SAO has begun follow-up testing. Those results will not be final until February 2016.		2/1/2016
<b>West Texas: A-133 Audit (performed by the SAO), Adams, Martin, Herrera</b>	1.	Summary: The College did not maintain adequate access controls over financial aid functions in Colleague.	A. Revoke access. B. Reduce administrator rights to only 3 individuals. C. Remove the ability for programmers to migrate code to the production environment. D. Require mandatory account reviews, and sample accounts to ensure access is appropriate.	<b>06/08/15:</b> SAO has begun follow-up testing. Those results will not be final until February 2016.		2/1/2016
<b>Marshall: A-133 Audit (performed by the SAO), Sanders, Adams, Herrera</b>	1.	Summary: Cost of Attendance budgets need to be adjusted to reflect actual enrollment so that the potential for over awards is reduced.	Continue to run an automated process to adjust awards based upon enrollment. The financial aid office will ensure only eligible budget components are included in the COA calculation.	<b>06/08/15:</b> SAO has begun follow-up testing. Those results will not be final until February 2016.		2/1/2016
	2.	Automated controls do not ensure Pell and loan awards are not changed manually.	A report will be run to ensure all awards are appropriate.	<b>06/08/15:</b> SAO has begun follow-up testing. Those results will not be final until February 2016.		2/1/2016
	3.	Summary: The College did not maintain adequate access controls over financial aid functions in Colleague.	A. Revoke access. B. Reduce administrator rights to only 3 individuals. C. Remove the ability for programmers to migrate code to the production environment. D. Require mandatory account reviews, and sample accounts to ensure access is appropriate.	<b>06/08/15:</b> SAO has begun follow-up testing. Those results will not be final until February 2016.		2/1/2016

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
Waco: Safety & Security Audit (15-012A), Wolaver	1.	We identified four areas we feel warrant management's consideration.	The Waco management team provided comprehensive and detailed responses to the areas we noted.	<b>Substantially Complete:</b> Performed a follow-up on 06/09/15. Found that most of outstanding items noted in the report were addressed. Management is currently addressing the other areas. This audit should clear from the schedule on the due date.		8/31/2015
West Texas: Skills Development Fund Grant Audit (15-006A), Hyde	1.	We identified several exceptions related to this specific grant that should be addressed prior to it being closed out. Going forward, the processes which allowed these exceptions to occur should be enhanced.	1.1 All reporting errors will be corrected before the grant is closed out. 1.2 All credit will be awarded to course completers before the grant is closed out. 1.3 Going forward, we will ensure all contracts are properly executed. 1.4 Request a grant extension.	<b>On-going:</b> 40 trainees thought to be non-completers were designated by TWC as completers because they finished over 50% of the training; Documentation is being gathered from 3rd party trainers who were paid without sufficient paperwork to justify the payments, with training occurring to prevent recurrence; The grant has been extended to 09/30/15 with hopes that it can be extended to April 2016; One new company has been secured to participate in training; A contract extension request will be submitted in August to request the April 2016 extension, addition of the new company, additional equipment purchases, and correction of course hours.		12/31/2015
Ft. Bend: Safety & Security Audit (15-027A), Wolaver	1.	We identified two areas we feel warrant management's consideration.	The Harlingen management team provided comprehensive and detailed responses to the areas we noted.	<b>On-going:</b> The completion of the outstanding items were transferred to the Harlingen team. We fully expect this to be completed by the due date.		8/31/2015
Hutto: Safety & Security Audit (15-032A), Wolaver	1.	We identified one area we feel warrants management's consideration.	The Waco management team provided comprehensive and detailed responses to the areas we noted.	<b>Substantially Complete:</b> Performed a follow-up on 06/09/15. Found that most of outstanding items noted in the report were addressed. Management is currently addressing the other areas. This audit should clear from the schedule on the due date.		8/31/2015

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: VA Benefits Compliance Audits (15-029A & 30A), Adams	1.	A centralized and standardized method for maintaining and monitoring documentation, and reporting enrollment data to the VA needs to be implemented. The processes currently on both campuses varies, with documentation and reporting exceptions noted at both.	<p>We will:</p> <ul style="list-style-type: none"> <li>- Centralize files that contain all required documents for every student by scanning all documents for safekeeping in ImageNow.</li> <li>- Because some offices do not have scanners, equipment will need to be purchased as resources permit.</li> <li>- All school certifying officials will begin using curriculum information obtained from the THECB to evaluate courses and programs of study.</li> <li>- Obtain access to required documents maintained by other departments and determine a way to organize these.</li> </ul> <p>We feel these steps will help us better meet monitoring and reporting requirements.</p>	Pending Review		Immediately
Marshall: Safety & Security Audit (15-033A),	1.	We identified one area we feel warrants management's consideration.	The Marshall management team provided comprehensive and detailed responses to the areas we noted.	On-going		8/31/2015
North Texas: Safety & Security Audit (15-035A), Rowland	1.	We identified one area we feel warrants management's consideration.	The North Texas management team provided comprehensive and detailed responses to the areas we noted.	On-going		8/31/2015
OIT: External Network Penetration Test (15-043A) performed by MainNerve, Herrera	1.	A TSTC web site was vulnerable to a SQL injection attack. MainNerve executed the SQL injection and subsequently retrieved student registration data, including full names, home addresses, email addresses, and telephone numbers. Other data of interest included TSTC staff-related information that contained contact information and work roles.	The site www.waco.tstc.edu was found to be vulnerable to SQL injection. The code that allowed this was immediately isolated and removed. Our Information Security personnel validated the correction by attempting to repeat the injection without success. Additionally, on July 1st 2015 the Waco.tstc.edu site will be deactivated in favor of the single tstc.edu website. We consider this item resolved, however, MainNerve will verify our assertion in follow-up testing.	Pending Review		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
	2.	There are many systems exposed to the Internet with services that could be accessed and enumerated easily using clear text protocols, such as SNMP. By exploiting this misconfiguration, MainNerve downloaded specific details regarding the target system. Most of the systems detected were printers whose value lay in the fact that the internal IP address was disclosed. This information allows an attacker to profile the internal network for potential future attacks. MainNerve also connected to several printers sent print commands.	The ability to access select printers via the internet has never been an intended practice. We have eliminated the ability to access through the internet the specific printers identified by MainNerve. We are currently unaware of any printers with the same vulnerability, but will immediately eliminate the risks if they present themselves in the future. We consider this item resolved, however, MainNerve will verify our assertion in follow-up testing.	Pending Review		Immediately
	3.	Various Polycom telecom systems were detected with some being video enabled. Unauthenticated telnet sessions was permitted on one system wherein remote dialing over POTS (Plain Old Telephone System) call to a MainNerve facility was possible.	MainNerve was able to utilize default vendor credentials to access a video conferencing device, and were able to make phone calls from the device. We will remove the default credentials. This will also be verified in the upcoming MainNerve follow-up testing.	Pending Review		Immediately
	4.	A host containing a critical vulnerability related to MS14-066 which could allow remote code execution by a remote user. MainNerve attempted to exploit this vulnerability on several occasions without success.	MainNerve detected and successfully exploited the Heartbleed vulnerability on a video conference type device in Harlingen. We updated the software which allowed this vulnerability, and will continue to work with all vendors to ensure software/firmware is always up to date. We consider this item resolved, however, MainNerve will verify our assertion in follow-up testing.	Pending Review		Immediately
	5.	A system containing critical vulnerabilities related to the Novell eDirectory software was detected on a different TSTC web site.	Four SMTP servers discovered by MainNerve send emails from limited internal devices and applications. Even though SMTP servers are publicly visible, and our security safeguards were able to restrict MainNerve from doing anything. We consider this issue properly controlled.	Pending Review		Immediately



**Internal Audit Department**

**Audit Report**

**Safety & Security Audit  
of  
TEXAS STATE TECHNICAL COLLEGE  
Breckenridge Campus**

**May 22, 2015**

**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

### Table of Contents

Executive Summary .....	1-2
Introduction.....	2
Objectives .....	2
Scope & Methodology .....	2-3
General Observations.....	3
Summary of Finding .....	3
Opinion .....	3-4

Internal Audit completed a comprehensive audit of safety and security policies and processes at the Breckenridge campus of TSTC as of April 30, 2015.

The purpose of the audit was to verify the existence of comprehensive policies and procedures that assist with

protecting both students and employees. Because of the numerous risks the campus faces, we utilized checklists developed by the Texas School Safety Center for use by community colleges. Community colleges are required by TEC 37.108(b) to conduct and report a safety audit every 3 years. While this regulation does not specifically apply to TSTC, the checklist is relevant.

We tested the following areas in this audit:

- Behavioral assessment/correction policies and procedures,
- Physical characteristics of all facilities (instructional and administrative) which affect safety/security,
- Fire/emergency responder related issues,
- Alarms, security cameras, emergency phones, and panic buttons,
- Landscaping,
- Access controls to facilities,
- Police/security policies and procedures,
- Emergency Management/Business Continuity policies and procedures,
- Lab safety for students and employees,
- Transportation safety and related policies,
- Other general policies and procedures that have been implemented to achieve safety (sexual harassment/assault, timely warning, emergency closing, etc.), and
- Emergency communications processes.

We conducted observations in the 3 instructional/administrative buildings. There are no residential facilities or culinary facilities.

Based on our audit work, we feel the campus has developed and put into place comprehensive and robust safety measures. A detailed list of our positive observations is located in the general observations section of this report.

We offered a few recommendations as enhancements to existing procedures. Because these recommendations did not represent significant deficiencies, we felt that they did not warrant being communicated in detail to the Board. For example, we made recommendations to management to better maintain first aid kits in all buildings, consider robbery procedures and training for cashiers, replace door handles that can be chained (as resources permit), and to mount two fire extinguishers that were not mounted on the wall. We also recommended that safety concerns throughout the campus community be gauged periodically, and that vehicle keys be better controlled.

## Introduction

Campus safety and security is the single most important objective at any educational institution. Without adequate safety processes, all other objectives are put at risk.

TSTC Breckenridge is comprised of three building in downtown Breckenridge. Collectively, there are dozens of employees, students, and visitors on the campus on a daily basis. The technologies taught at TSTC pose inherent safety risks to both employees and students. Given the risks that exist, it is impossible to list, let alone address, all of them. Nevertheless, the campus has implemented a comprehensive safety program that employs monitoring, education, and policies. The Breckenridge Police Department is within minutes of the campus. The Fire Department is directly across the street.

## Objectives

The objectives of the audit were to ensure student and employee safety and security are being achieved on the Breckenridge campus, and that policies and procedures are in place to ensure on-going safety.

## Scope & Methodology

The scope of our audit included all safety related policies and procedures, physical characteristics of all buildings, instructional lab practices, police department practices, crime and fire reports, emergency communication procedures, and food safety practices. Given the infinite number of safety risks that exists, this audit was not intended to verify all risks. It was intended to identify common ones that are known to exist on this campus and institutions of higher education in general.

To accomplish our objectives, we utilized a safety checklist developed by the Texas School Safety Center. It addressed

common risks found on institutions of higher education. It was developed using numerous State and Federal resources. Our method of testing primarily consisted of observation, inquiry, and policy review. We also inquired about the handling of all sexual assaults reported on the 2014 Campus Crime report. [NOTE: None were reported in West Texas].

## General Observations

We observed numerous positive practices that help ensure safe and secure campuses. The following is a list of several of them:

- The campuses actively monitor its safety performance and stress the importance of safety to employees and students.
- Instructors are enforcing protective equipment and safety practices in labs. Additionally, safety training is conducted prior to students engaging in labs.
- Fire extinguishers are deployed throughout the campuses.
- Locked doors and key tracking procedures are in place.
- 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.
- Comprehensive safety related policies are in place. Some of the more extensive ones include a Business Continuity Plan, Sexual Assault and Harassment Policies, Personal Protective Equipment Policy, and a policy on the Campus Security Act.
- An annual Campus Safety Report is prepared and published. The report lists certain reported crimes that occurred on the campus.
- Artificial defibrillator devices (AED's) are deployed in some buildings and management is considering purchasing additional AED's.
- We noted an overwhelming attitude and awareness of safety throughout the campus, particularly with staff and instructors.
- The State Office of Risk Management also recently reviewed the campus and did not note any issues.

## Summary of Finding

No reportable issues were found.

## Opinion

Based on the audit work performed, the campus has implemented appropriate safety and security practices to ensure students and employees are reasonably safe. In my opinion, the campus is not only safe, but has the appropriate procedures in place to ensure it remains that way.



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

Submitted by:

A handwritten signature in black ink, appearing to read "Jason D. Mallory", is written over a horizontal line.

Jason D. Mallory, CPA, CIA

May 22, 2015

Date



**Internal Audit Department**

**Audit Report**

**Safety & Security Audit  
of  
TEXAS STATE TECHNICAL COLLEGE  
Brownwood Campus**

**May 22, 2015**

**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

### Table of Contents

Executive Summary .....	1-2
Introduction.....	2
Objectives .....	2
Scope & Methodology .....	2-3
General Observations.....	3
Summary of Finding .....	3
Opinion .....	3-4

Internal Audit completed a comprehensive audit of safety and security policies and processes at the Brownwood campus of TSTC as of April 30, 2015.

The purpose of the audit was to verify the existence of comprehensive policies and procedures that assist with

protecting both students and employees. Because of the numerous risks the campus faces, we utilized checklists developed by the Texas School Safety Center for use by community colleges. Community colleges are required by TEC 37.108(b) to conduct and report a safety audit every 3 years. While this regulation does not specifically apply to TSTC, the checklist is relevant.

We tested the following areas in this audit:

- Behavioral assessment/correction policies and procedures,
- Physical characteristics of all facilities (instructional and administrative) which affect safety/security,
- Fire/emergency responder related issues,
- Alarms, security cameras, emergency phones, and panic buttons,
- Landscaping,
- Access controls to facilities,
- Police/security policies and procedures,
- Emergency Management/Business Continuity policies and procedures,
- Lab safety for students and employees,
- Transportation safety and related policies,
- Other general policies and procedures that have been implemented to achieve safety (sexual harassment/assault, timely warning, emergency closing, etc.), and
- Emergency communications processes.

We conducted observations in the 3 instructional/administrative buildings. There are no residential facilities or culinary facilities.

Based on our audit work, we feel the campus has developed and put into place comprehensive and robust safety measures. A detailed list of our positive observations is located in the general observations section of this report.



We offered a few recommendations as enhancements to existing procedures. Because these recommendations did not represent significant deficiencies, we felt that they did not warrant being communicated in detail to the Board. For example, we made recommendations to management to better maintain first aid kits in all buildings, consider robbery procedures and training for cashiers, and to replace door handles that can be chained (as resources permit). We also recommended that safety concerns throughout the campus community be gauged periodically.

## Introduction

Campus safety and security is the single most important objective at any educational institution. Without adequate safety processes, all other objectives are put at risk.

TSTC Brownwood is comprised of three building in downtown Brownwood. Collectively, there are dozens of employees, students, and visitors on the campuses on a daily basis. The technologies taught at TSTC pose inherent safety risks to both employees and students. Given the risks that exist, it is impossible to list, let alone address, all of them. Nevertheless, the campus has implemented a comprehensive safety program that employs monitoring, education, and policies. Brownwood Police and Fire Departments are within minutes of the campus. Additionally, a State law enforcement agency is housed in building 2 of the campus.

## Objectives

The objectives of the audit were to ensure student and employee safety and security are being achieved on the Brownwood campus, and that policies and procedures are in place to ensure on-going safety.

## Scope & Methodology

The scope of our audit included all safety related policies and procedures, physical characteristics of all buildings, instructional lab practices, police department practices, crime and fire reports, emergency communication procedures, and food safety practices. Given the infinite number of safety risks that exists, this audit was not intended to verify all risks. It was intended to identify common ones that are known to exist on this campus and institutions of higher education in general.

To accomplish our objectives, we utilized a safety checklist developed by the Texas School Safety Center. It addressed common risks found on institutions of higher education. It was

developed using numerous State and Federal resources. Our method of testing primarily consisted of observation, inquiry, and policy review. We also inquired about the handling of all sexual assaults reported on the 2014 Campus Crime report. [NOTE: None were reported in West Texas].

## General Observations

We observed numerous positive practices that help ensure safe and secure campuses. The following is a list of several of them:

- The campuses actively monitor its safety performance and stress the importance of safety to employees and students.
- Instructors are enforcing protective equipment and safety practices in labs. Additionally, safety training is conducted prior to students engaging in labs.
- Fire extinguishers are deployed throughout the campuses.
- Locked doors and key tracking procedures are in place.
- 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.
- Comprehensive safety related policies are in place. Some of the more extensive ones include a Business Continuity Plan, Sexual Assault and Harassment Policies, Personal Protective Equipment Policy, and a policy on the Campus Security Act.
- An annual Campus Safety Report is prepared and published. The report lists certain reported crimes that occurred on the campus.
- Artificial defibrillator devices (AED's) are deployed in some buildings and management is considering purchasing additional AED's.
- We noted an overwhelming attitude and awareness of safety throughout the campus, particularly with staff and instructors.
- The State Office of Risk Management also recently reviewed the campus and did not note any issues.

## Summary of Finding

No reportable issues were found.

## Opinion

Based on the audit work performed, the campus has implemented appropriate safety and security practices to ensure students and employees are reasonably safe. In my opinion, the campus is not only safe, but has the appropriate procedures in place to ensure it remains that way.

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



Submitted by:

A handwritten signature in black ink, appearing to read "Jason D. Mallory", is written over a horizontal line.

Jason D. Mallory, CPA, CIA

May 22, 2015

Date



**Internal Audit Department**

**Audit Report**

**VA Benefits Compliance Audit  
of  
TEXAS STATE TECHNICAL COLLEGE  
Harlingen & Waco Campuses**

**June 23, 2015**

**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

### Table of Contents

Executive Summary .....	1
Introduction.....	1-2
Objectives .....	2
Scope & Methodology .....	2
General Observations.....	2-3
Summary of Finding .....	3
Opinion .....	3
Audit Finding Detail.....	4-5

Internal Audit has completed compliance audits of VA benefits awarded to students in Harlingen and Waco from September 2013 through December 2014. The purpose of the audits was to ensure the College facilitated the awards by following the appropriate guidelines outlined in the School Certifying Official Handbook published by the U.S. Department of

Veteran's Affairs (Handbook).

We tested benefit payments made directly to the College, required employee training, tuition/fees policies and marketing efforts, and records security. Most of our audit consisted of verifying courses students took were within their approved programs of study, that required documentation was maintained, and that academic progress and enrollment activity was appropriately monitored and reported to the Department of Veterans Affairs (VA) accurately and timely.

Through our testing we determined payments are being applied correctly, records and associated information are reasonably secured, and all employees that handle VA Benefits have been properly certified and trained. We also did not identify any prohibitive tuition practices or deceptive marketing efforts that negatively impact veterans.

The one area we feel needs to be addressed affects documentation and reporting requirements. We identified sufficient documentation and reporting exceptions to indicate, in our opinion, the College would benefit from improving and standardizing those processes across each campus.

## Introduction

Each campus has a dedicated VA office that facilitates VA benefits for students who qualify for them. Both campuses have a Veteran's Center which was funded by grants. Until July 2013, the VA office in Harlingen was part of the Financial Aid Office (FA), with VA and FA staff supporting VA students. FA still provides assistance when the VA staff needs help. Waco has always been a stand-alone function, but has expanded in recent months.

The VA, not the College, initially qualifies students for federal benefits after the students complete an application for the

benefits. The VA approves that application using the military service records they have of the students, and then sends the student a certificate of eligibility who then presents it to the College. The College is responsible for certifying student's courses of study to the VA, maintaining required documentation, and reporting academic and enrollment standing so that the VA can determine continued eligibility.

In the Spring of 2015, the Waco campus had 396 students receiving VA benefits, and the Harlingen campus had 276 students. During this audit, the VA offices at the campuses were reorganized under the direction of one lead supervisor. Those areas fall within the Operations Division under the AVC/Executive - Student Development.

There are several VA educational benefits being used by students, with the most common one being Chapter 33 (commonly referred to as the Post-911 GI Bill).

## Objectives

The purpose of the audit was to verify the College complied with the major requirements listed in the Handbook. Specifically, we verified payments were correct, employees were properly trained, tuition/fees policies and marketing efforts are not prohibitive or deceptive, and related records and information are reasonably secured. A significant portion of our audit was aimed to verify that awards facilitated by the College were supported by required documentation and academic monitoring, and that communication to the VA was accurate and timely.

## Scope & Methodology

The scope of our audit included all federal VA benefits awarded to students during the period of September 2013 through December 2014. We developed our audit criteria using the Handbook published by the U.S. Department of Veteran's Affairs. Our methods consisted primarily of verifying required documentation was maintained, accurate, and timely. We also traced payments of benefits to ensure their appropriate disbursement, reviewed marketing practices, validated training of employees, and verified the security of physical and electronic records that contained sensitive information.

## General Observations

In both offices, we saw employees (some who are themselves veterans) striving to support student needs. We noted that each campus is actively trying to grow its veteran enrollment. There has been a steady increase of veterans being served. In Waco,

veterans increased from 360 in fall 2012 to 461 in fall 2014. In Harlingen, for the same time period, veterans served increased from 261 to 308. Additionally, the VA offices not only assist with educational benefits, but provide an environment where veterans can interact with other veterans.

### Summary of Findings

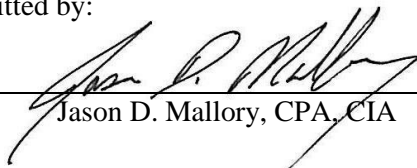
A centralized and standardized method for maintaining and monitoring documentation, and reporting enrollment data to the VA needs to be implemented. The processes currently on both campuses varies, with documentation and reporting exceptions noted at both.

### Opinion

Based on the audit work performed, payments are being applied correctly, records and associated information are reasonably secured, and all employees that handle VA Benefits have been properly certified and trained. We also did not identify any prohibitive tuition practices or deceptive marketing efforts that negatively impact veterans. We did find, however, that documentation and reporting processes need to be standardized and improved.

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

Submitted by:



Jason D. Mallory, CPA, CIA

23 June 2015

Date

---

**AUDIT FINDING DETAIL**

---

Finding #1: A centralized and standardized method for maintaining and monitoring documentation, and reporting enrollment data to the VA needs to be implemented. The processes currently on both campuses varies, with documentation and reporting exceptions noted at both.

**Criterion:** The School Certifying Official Handbook published by the U.S. Department of Veteran's Affairs requires the College to maintain specific records on each student receiving federal veteran's educational benefits so that the College can verify eligibility and notify the VA of pertinent changes in the student's academic and/or enrollment status. And, while not required, the Handbook strongly encourages schools to maintain files to store those records, and even goes as far as describing the order that the records should be maintained in the file. The Handbook also requires the College to certify courses taken by the student are part of an approved academic program, and requires notification within 30 days of enrollment or enrollment changes.

In both Harlingen & Waco, we determined that physical files on students were maintained to varying degrees. For documents that were not maintained in the files, we were generally able to find them in the files of other College departments, Colleague, or the electronic files of the VA office.

We noted that the record keeping methods varied not only within the same office on the same campus, but also between campus offices. The causes of these seem to be due to employee turnover, and the fact that the campuses and management were historically separate. But as a result of single accreditation, management since January 2015 has been actively involved in identifying and resolving such difference.

In our testing, there were instances where we did not find required documentation in the VA files nor in files of other College departments. We also found instances where courses were taken that were not part of the approved program of study for the student, and instances where enrollment certifications and changes were not timely reported. While these exceptions were not widespread, we found enough for us to feel they are direct results of not maintaining records in a standardized format in a central location. The VA has presumably recommended the standardized file system because it assists with meeting records keeping guidelines, and ensures the records are actually being reviewed by the College's VA representatives. Even though we were able to find most of the documents and information (whether in the VA offices or other College departments), because some of that information was found outside of the VA offices we cannot give assurance that the information is always being reviewed by our VA representatives.

**Consequences:** Not meeting VA documentation, monitoring and reporting requirements. Potential to not satisfy VA records retention requirements.

**Possible Solution:** Maintain, in either physical or electronic form, centralized files on every student which contain all the required documents listed in the VA Handbook. We recommend using the format suggested in the Handbook. This would expedite inquiries from internal and VA auditors, help ensure the College is actually meeting its monitoring and reporting requirements,



and ensure records retention requirements are not impacted by the actions of other College departments.

**Management Response:**

**Division:** Student Development

**Senior Management:** Mary Adams

Task	Brief Description	Responsible Individual	Completion Date
1.1	<p>We will:</p> <ul style="list-style-type: none"><li>- Centralize files that contain all required documents for every student by scanning all documents for safekeeping in ImageNow.</li><li>- Because some offices do not have scanners, equipment will need to be purchased as resources permit.</li><li>- All school certifying officials will begin using curriculum information obtained from the THECB to evaluate courses and programs of study.</li><li>- Obtain access to required documents maintained by other departments and determine a way to organize these.</li></ul> <p>We feel these steps will help us better meet monitoring and reporting requirements.</p>	Steve Guevara	Immediately



**Internal Audit Department**

**Self-Assessment Report**

**Internal Quality Assurance Review  
of  
TEXAS STATE TECHNICAL COLLEGE  
Internal Audit**

**February 27, 2015**

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

## OVERALL CONCLUSION

After completing the self-assessment for our April 2015 peer review, our conclusion is that the TSTC Internal Audit function **is in compliance with** *The IIA Standards for the Professional Practice of Internal Auditing*, the U.S. Government Accountability Office's *Government Auditing Standards*, the IIA Code of Ethics, and the Texas Internal Auditing Act. Our conclusion is based on our completion of self-assessment tools developed by the State Agency Internal Audit Forum (SAIAF). As part of our commitment to continuous improvement, during the self-assessment we identified opportunities to enhance our processes and documentation, and have detailed them in the final section of this report entitled "Opportunities for Improvement."

More detail regarding our self-assessment is found below. It includes an assessment of compliance with *The IIA Code of Ethics*, followed by eleven sections presented in the order of *The IIA Standards*.

## DETAILED CONCLUSIONS

### **IIA Code of Ethics**

The Internal Audit Charter documents the expectation that auditors conform to the IIA Code of Ethics. Also, the Internal Audit Policies and Procedures specify that all staff abide by the Code of Ethics. In addition, each auditor acknowledges their responsibilities in an annual confirmation process.

### **I. 1000 Purpose, Authority, and Responsibility**

The purpose, authority and responsibility of Internal Audit are specified in the Internal Audit Charter. It defines the nature of assurance and consulting services. It has been approved by the Board of Regents, and is reviewed annually to ensure it meets current needs.

### **II. 1100 Independence and Objectivity**

Internal Audit is independent and free from impairments, and its staff is objective in performing their work. The Director of Audits (Director) reports functionally to the Audit Committee of the Board of Regents, with administrative functions being approved by the Chancellor. That reporting structure is approved within the Internal Audit Charter. The Board of Regents reviews and approves the Annual Audit Plan and all significant deviations from it. They receive copies of all audit reports before they are issued to the State Auditor's Office, Sunset Advisory Commission, Governor's Office, and Legislative Budget Board. Internal Audit has not experienced any scope limitations and has been able to report all findings and conclusions objectively without interference from management. No conflicts of interest have occurred, yet the division has a process for addressing such situations should they arise.

## **II. 1200 Proficiency and Due Professional Care**

Assignments are performed with proficiency and due care; professional judgment is used in planning, performing, and reporting; and the staff collectively possesses adequate professional competencies. The Director holds a BBA in accounting, is a licensed Texas CPA, and holds certified internal auditor (CIA) and certified control self-assessment (CCSA) designations from the Institute of Internal Auditors (IIA). He has nineteen years of audit experience, including eight as an internal audit director. All of the internal auditors have business-related graduate or undergraduate degrees, and the staff is currently pursuing professional CIA certifications. Each staff member has at least 7 years of working in higher education. Other industry experiences include public accounting, banking, insurance, manufacturing, and aircraft. Over 44 years of auditing experience resides in the department. Audits are assigned according to the knowledge, skills, and experience of the auditors. A risk assessment is performed for each audit, with IT and fraud risks being considered in each. The departmental budget provides funding for all personnel to earn continuing education credits and to pursue certifications. The department also maintains a professional resources library, and is a member of both the IIA and the Association of College and University Auditors (ACUA). Finally, the Director attends monthly Executive Management Council meetings to maintain an awareness of current strategic initiatives.

## **IV. 1300 Quality Assurance and Improvement Program**

An effective quality assurance program exists which includes external peer reviews and other periodic internal review processes. The Director approves individual audit plans and audit programs, as required by internal policies and procedures. All working papers are reviewed by the Director prior to a report being issued, and he also approves all audit reports. Quality control meetings are held monthly with the entire staff, as well as frequent (often daily) one-on-one meetings with each staff. Internal customer surveys are sent to auditees after audits are completed. Audit reports state that audits are performed in accordance with *Standards*.

## **V. 2000 Managing the Internal Audit Activity**

Internal Audit is managed in accordance with relevant *Standards*. All staff has been issued an Internal Audit Policies and Procedures manual, with that manual being reviewed annually. The Director prepares a risk-based Annual Audit Plan that is approved by the Board of Regents; monitors and communicates the progress of projects; coordinates with other audit entities to prevent duplication; and prepares an Annual Report on Internal Audit. Audit reports provide value-added recommendations to address the issues that are identified. Follow-up reviews add value by informing management of the status of audit issues identified in previous reports.

## **VI. 2100 Nature of Work**

Internal Audit contributes to the improvement of risk management, control, and governance processes through its audits and management assistance services. Internal Audit performs a College-wide annual risk assessment that forms the basis for the Annual Audit Plan. This risk assessment incorporates input from the Executive Management Council and Board of Regents, and considers risks common to other Texas higher educational institutions. Risk exposures considered

in the assessment include asset liquidity/fraud, regulatory compliance, financial statement impact, importance of information, customer impact, and changes in processes. Specific fraud risks are considered in each audit. The Director has provided input on ethics and fraud prevention policies.

#### **VII. 2200 Engagement Planning**

Audit plans are developed during each audit. Those plans specify the audit scope and objectives. An audit program is prepared for each audit that identifies the activities to be performed in order to accomplish the audit objectives. The Director assigns audits according to the knowledge, skills, and experience of the auditors. Comprehensive planning documentation is created that demonstrates sufficient knowledge is gained of areas under audit to ensure appropriate audit objectives are developed for the related risks.

#### **VIII. 2300 Performing the Engagement**

Thorough working papers document the audit program steps performed to achieve the audit objectives. Evidence provided to support results and conclusions is sufficient, competent, and relevant. Audits and consulting projects are properly supervised, and working papers are reviewed before reports are issued.

#### **IX. 2400 Communicating Results**

Written reports are prepared for all audits and consulting engagements. Audit reports include the objectives, scope, and methodology. The results are communicated to the appropriate internal and external parties, including executive management, program management, Board of Regents, the Governor's Office, State Auditor's Office, Legislative Budget Board, and the Sunset Advisory Commission. Management is provided an opportunity to review and discuss all audit reports prior to them being issued. Similarly, they are given the opportunity to formulate action plans (if applicable) to address recommendations made in the reports.

#### **X. 2500 Monitoring Progress**

An effective system for monitoring the disposition of results is in place and communicated to management and the Board of Regents. A "follow-up schedule" for tracking the status of issues identified in audit reports is maintained, and follow-up procedures are performed of previously unresolved issues. The Annual Audit Plan includes the follow-up reviews to be performed for the year. The results of follow-up reviews are communicated to executive and program management.

#### **XI. 2600 Resolution of Senior Management's Acceptance of Risks**

No instance has occurred in which the Director believes executive management has accepted a level of residual risk that is unacceptable to the organization, but if this

situation were to occur there is a process for reporting it to the Chancellor and the Board of Regents.

Submitted by:



---

Jason D. Mallory, CPA, CIA

February 27, 2015

---

Date

## **OPPORTUNITIES FOR IMPROVEMENT**

During our preparation of the self-assessment, we made some clarifications to our Internal Audit Policies and Procedures manual and also identified some improvements we will make to our practices &/or documentation. Those include:

- Working papers prepared by the Director of Audits are generally not reviewed by another member of the department prior to the issuance of the audit report. Going forward, those will be subject to review by another staff member. This will not only ensure consistency in the performance of the procedure, but will assist with quality control.
- Internal quality control procedures have not been reported annually to the Audit Committee. While adequate quality control procedures are in place, annual reporting of those procedures and their results will assure the Audit Committee that audit quality is being monitored for compliance to Standards.
- Current procedures for continuing professional education of all staff are not in compliance to GAGAS 3.76 & 3.78. The internal policy requires 40 hours to be obtained by auditors in a 2-year period, however, the Standards require 80 hours. Internal policy will be changed to reflect the 80 hour standard, and a more concerted effort will be given to achieve those hours.

The TSTC Internal Audit Department is committed to continuous improvement and ensuring the proficiency of all staff. We will continue to revisit and improve our practices and related documentation.



**Office of Internal Audits**

P.O. Box 425587, Denton, TX 76204-5587  
940-898-3260 Fax 940-898-2986

April 29, 2015

Mr. Jason Mallory  
Internal Audit Department  
Texas State Technical College  
3801 Campus Drive  
Waco, TX 76705

Dear Mr. Mallory,

At your request, we performed an external quality assurance review (EQAR) of the Texas State Technical College Internal Audit Department (TSTCIAD) to assess compliance with the following:

- Texas Internal Auditing Act (Tex. Gov't. Code Chapter 2102);
- Institute of Internal Auditors *Code of Ethics* and *International Standards for the Professional Practice of Internal Auditing*; and
- U.S. Government Accountability Office *Generally Accepted Government Auditing Standards*.

These are collectively referred to as the *Standards* for purposes of this review.

The EQAR was performed by Andrew Groover, Director of Internal Audits for Texas Woman's University and Leticia Charbonneau, Executive Director of Internal Audit for Lone Star College System, with onsite fieldwork conducted April 6<sup>th</sup> and 7<sup>th</sup> 2015.

The review was conducted in accordance with the State Agency Internal Audit Forum Peer Review Guidelines using the Master Peer Review Program. It included audit activities from September 2011 – January 2015.

**Rating System for Opinion**

The rating system that was used for expressing an opinion for this review provides for three levels of conformance: generally conforms, partially conforms, and does not conform.

- *Generally conforms* means that the TSTCIAD has policies, procedures, and an audit charter that were judged to be in accordance with applicable standards; however, opportunities for improvement may exist.
- *Partially conforms* means deficiencies, while they might impair, did not prohibit the TSTCIAD from carrying out its responsibilities.



- *Does not conform* means deficiencies in practice were found that were considered so significant as to seriously impair or prohibit the TSTCIAD in carrying out its responsibilities.

## **Introduction**

The Texas Internal Auditing Act requires TSTCIAD to conform to standards established by the Institute of Internal Auditors (IIA) and the U.S. Government Accountability Office (GAO). The *International Standards for the Professional Practice of Internal Auditing*, promulgated by the IIA, require external assessments to be performed at least once every five years by a qualified, independent reviewer or review team from outside the organization. The *Generally Accepted Government Auditing Standards* (GAGAS) issued by the GAO require an external assessment at least every three years. The Texas Internal Auditing Act also requires an external assessment every three years.

This report represents the results of the external quality assurance review that we conducted. The objectives were to assess the level of TSTCIAD's compliance with the *Standards* and identify opportunities to enhance its operations.

## **Scope**

The scope of the review included:

- Review of self-assessment materials prepared by the Director, including the audit charter, audit manual, and other organizational materials;
- Interviews with the Chair of the Audit Committee, TSTC Chancellor, Vice Chancellor for Finance, Vice Chancellor and Chief Information Officer; State Auditor's Office Audit Manager for TSTCIAD, Director of Internal Audits and Internal Audit Staff members in Waco and Harlingen.
- Examination of four sets of work papers and the related audit report produced by the TSTCIAD during the EQAR period; and
- A comparison of the TSTCIAD's audit practices with the *Standards*.
- A survey of various TSTC administrative staff.

## **Overall Opinion**

In our opinion, the Texas State Technical College Internal Audit Department ***generally conforms*** to the *Standards* for the period under review.

The following table contains our opinion of how the TSTCIAD activities conform to each section of the *International Standards for the Professional Practice of Internal Auditing*, IIA Code of Ethics, and Texas Internal Auditing Act. GAGAS areas are not specifically mentioned in the table but are similar to the *International Standards for the Professional Practice of Internal Auditing* attribute and performance standards. Recommendations for

areas of improvement for the TSTCIAD revealed as part of the EQAR process are included below.

<b>IIA Standard Type and Description</b>	<b>Opinion</b>
<b><i>Attribute Standards</i></b>	
1000 – Purpose, Authority, and Responsibility	Generally conforms
1100 – Independence and Objectivity	Generally conforms
1200 – Proficiency and Due Professional Care	Generally conforms
1300 – Quality Assurance and Improvement Program	Partially conforms
<b><i>Performance Standards</i></b>	
2000 – Managing the Internal Audit Activity	Generally conforms
2100 – Nature of Work	Generally conforms
2200 – Engagement Planning	Generally conforms
2300 – Performing the Engagement	Generally conforms
2400 – Communicating Results	Generally conforms
2500 – Monitoring Progress	Generally conforms
<b>IIA Code of Ethics</b>	Generally conforms
<b>Texas Internal Auditing Act</b>	Generally conforms

During both the self-assessment performed by TSTCIAD and our external assessment, opportunities for enhancement were noted by both parties. Given our opinion that policies and procedures were in compliance with the Standards, the recommendations below do not represent observations of material non-compliance.

**Recommendations identified by the TSTC Director of Internal Audit as a result of completing the self-assessment.**

**1300 – Quality Assurance and Improvement Program**

*The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.*

Working papers prepared by the Director of Audits are generally not reviewed by another member of the department prior to issuance of the audit report. Going forward, those will be subject to review by another staff member. This will not only ensure consistency in the performance of the procedure, but will assist with quality control.

**1320 – Reporting on the Quality Assurance and Improvement Program**

*The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board.*

Internal quality control procedures have not been reported annually to the Audit Committee. While adequate quality control procedures are in place, annual reporting of those procedures and their results will assure the Audit Committee that audit quality is being monitored for compliance to Standards.

### **1230 – Continuing Professional Development**

*Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.*

Current procedures for continuing professional education do not require each auditor to obtain at least 40 hours per year. The internal policy requires 40 hours to be obtained by auditors in a 2-year period; however, the above standard is interpreted to mean 40 hours each year as a best practice. Internal policy will be changed to reflect the 40 hour standard and a more concerted effort will be given to achieve those hours.

***The EQAR team concurs with the recommendations identified by the self-assessment.***

### **Recommendations identified by the External Quality Assurance Review Team**

#### **1311 – Internal Assessments**

*Internal assessments must include:*

- *Ongoing monitoring of the performance of the internal audit activity; and*
- *Periodic self-assessments or assessments by other persons within the organization with sufficient knowledge of internal audit practices.*

Ongoing monitoring of the performance of the internal audit activity is being conducted; however, periodic self-assessments should be completed more frequently to enhance compliance with the Standards. The only self-assessment that was conducted during the EQAR period was the one completed for the EQAR.

#### **2110 – Governance**

***2110.A1 – The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.***

In reviewing the Annual Audit Plans for FY 2013, FY 2014, and FY 2015 and related progress reports we noted that there was no audit scheduled or completed to evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities. An audit of TSTC's ethics program should be conducted periodically to enhance compliance.

***2110.A2 – The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.***

In reviewing the Annual Audit Plans for FY 2013, FY 2014, and FY 2015 and related progress reports, we noted that there was no audit scheduled or completed to assess whether the information technology governance of the organization supports the organization's strategies and objectives. An audit of TSTC's information technology governance should be conducted periodically to enhance compliance.

**Texas Government Code Section 2102.005. INTERNAL AUDITING REQUIRED**

*A state agency shall conduct a program of internal auditing that includes:*  
*(2) periodic audits of the agency's major systems and controls, including:*  
*(C) electronic data processing systems and controls.*

In reviewing the audit plans for FY 2013, FY 2014, and FY 2015 and related progress reports we noted that comprehensive IT audit coverage can be enhanced. The TSTCIAD should increase audit coverage to ensure periodic audits of major systems such as Colleague, learning management systems, and the required audit of Texas Administrative Code 202 (required every two years) are conducted. In discussions with administration and staff, there was a common theme that IT audit coverage should be increased. This could be accomplished by the addition of an IT Auditor position to the department.

We appreciate the opportunity to conduct the EQAR of the TSTCIAD. We confirm that we are independent and have no actual or potential conflicts of interest associated with the TSTCIAD.

Sincerely,



Andrew S. Groover, M.Ed., CPA, CIA, CICA, CISA, CFE  
Director of Internal Audits  
Texas Woman's University



Leticia T. Charbonneau, CPA, CIA, CGAP  
Executive Director-Internal Audit  
Lone Star College System

cc:

Regent Ellis M. Skinner II, Chair  
Regent Joe M. Gurecky, Vice Chair  
Regent Linda McKenna  
Regent Penny Forrest  
Regent Ivan Andarza  
Regent John K. Hatchel  
Regent Joe K. Hearne  
Regent Keith Honey  
Regent James Virgil (J.V.) Martin  
Chancellor Mike Reeser



3801 Campus Dr. | Waco, TX 76705  
[www.tstc.edu](http://www.tstc.edu)

Office of Internal Audit  
254.867.3999  
Fax: 254.867.3912

April 29, 2015

Mr. Joe Gurecky, Audit Committee Chair  
Texas State Technical College System  
Waco, Texas 76705

Mr. Gurecky:

SUBJECT: Response to the Recommendations offered in the 2015 External Quality Assessment Review

I have formulated responses to the recommendations offered in the Internal Quality Self-Assessment conducted by me and the External Quality Assessment Review conducted by Andrew Groover of Texas Woman's University and Leticia Charbonneau of Lonestar Colleges.

As noted in both reports, the TSTC Internal Audit Department achieved the highest rating possible of "generally conforms to the standards." Those standards include the *International Standards for the Professional Practice of Internal Auditing* issued by the IIA, *Generally Accepted Government Auditing Standards* (GAGAS) issued by the GAO, and the Texas Internal Auditing Act.

Both of those audits resulted in recommendations for my consideration. While the recommendations are intended simply as opportunities to enhance my current processes and are not compliance related, I formulated responses so that you could be aware of my planned actions.

Sincerely,

A handwritten signature in black ink, appearing to read "Jason D. Mallory", is written over a light gray, stylized graphic of a star and curved lines.

Jason D. Mallory  
Director of Audits

**Division:** Internal Audit

**Senior Management:** Jason Mallory, Director of Audits

Task	Brief Description	Responsible Individual	Completion Date
1.1	The working papers prepared by the Director will be reviewed by another person in the Department.	Tahlia Pena	Immediately
1.2	An annual report to the Board will be prepared that lists the quality control procedures that are in place over the internal audit process.	Jason Mallory	August 13, 2015
1.3	I did not realize the different standards conflicted on this requirement. In practice everyone in the Department has obtained close to 40 hours or more of education annually, however our departmental policy only requires 20 hours. That policy will be updated to require at least 40 hours annually rather than 20.	Tahlia Pena	Immediately
1.4	The standards only require <u>periodic</u> self-assessments, which we perform. The term “periodic” is not defined. But to further demonstrate our commitment to quality, we will begin performing and documenting a self-assessment every 1.5 years, and reporting the results to the Board.	Tahlia Pena	Immediately
1.5	The ethics and IT governance audit recommendation implies that performing specific audits every 3 years is a requirement. But in fact compliance guidance included in the actual standards clearly state that we must be familiar with these processes, and that an understanding is most likely obtained through several different audits and processes. We will include these individual audits in our annual audit planning process, and perform them only if the risk rating is high in comparison to other auditable areas.	Jason Mallory	Immediately
1.6	In the past, specific IT audits similar to those listed in the peer review team’s recommendation were performed because a dedicated IT auditor was on staff. After losing that resource, we have gradually been rebuilding that capacity through training and outsourcing, and will continue down that path. In 2015, four specific IT audits were scheduled which demonstrates our commitment to performing IT audits. Going forward, IT specific audit will continue to be included in the annual audit plan.	Jason Mallory	Immediately



**Internal Audit Department**

**Audit Report**

**Safety & Security Audit  
of  
TEXAS STATE TECHNICAL COLLEGE  
Marshall Campus**

**June 15, 2015**

**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

### Table of Contents

Executive Summary .....	1-2
Introduction.....	2-3
Objectives .....	3
Scope & Methodology .....	3
General Observations.....	3-4
Summary of Finding .....	4
Opinion .....	4
Audit Finding Detail.....	5

Internal Audit completed a comprehensive audit of safety and security policies and processes at the Marshall campus of TSTC as of May 31, 2015.

The purpose of the audit was to verify the existence of comprehensive policies and procedures that assist with protecting both students and employees.

Because of the numerous risks the campus faces, we utilized checklists developed by the Texas School Safety Center for use by community colleges. Community colleges are required by TEC 37.108(b) to conduct and report a safety audit every 3 years. While this regulation does not specifically apply to TSTC, the checklist is relevant.

We tested the following areas in this audit:

- Behavioral assessment/correction policies and procedures,
- Physical characteristics of all facilities (instructional, administrative, residential) which affect safety/security,
- Fire/emergency responder related issues,
- Alarms and security cameras,
- Landscaping,
- Access controls to facilities,
- Police policies and procedures,
- Emergency Management/Business Continuity policies and procedures,
- Lab safety for students and employees,
- Transportation safety and related policies,
- Other general policies and procedures that have been implemented to achieve safety (sexual harassment/assault, timely warning, emergency closing, etc.), and
- Emergency communications processes.

We conducted observations in 6 instructional and administrative buildings, 1 multipurpose building, student residence facilities, and police operations.

Based on our audit work, we feel the campus has developed and put into place comprehensive and robust safety measures. Some examples include having at least one Security Officer on duty 24/7, having employees participate in First Aid/CPR training every 2 years, and the implementation of numerous safety related policies and procedures.



A more detailed list of our positive observations is located in the general observations section of this report.

Because of the number of procedures in this audit, we identified some areas that needed attention. Most of these observations were simply overlooked by management and were relatively minor, so we made recommendations in that regard. For example, we observed some metal shavings left on the equipment and floor in a lab, some areas that needed better lighting, and instances where evacuation routes and other safety related information was not posted. These observations were isolated occurrences in individual buildings, can be easily remedied, and/or did not represent issues pervasive throughout the entire campus. We felt that these observations did not warrant being communicated in detail to the Board given their nature. Rather, we gave this list to the management team to address.

## Introduction

Campus safety and security is the single most important objective at any educational institution. Without adequate safety processes, all other objectives are put at risk.

TSTC's Marshall campus encompasses approximately 72 acres of land that holds 5 instructional/administrative buildings, 1 multi-use facility (pavilion), 1 building leased from MEDCO (Marshall Economic Development Corp.), and 8 student residential facilities totaling 54 units, which includes 1 and 2 bedroom units. At full capacity, units can house 202 students. There are a couple hundred employees, students, and visitors on campus on a daily basis. The campus is located off of Highway 59, and approximately 2 miles from Interstate 20.

The technologies taught at TSTC pose inherent safety risks to both employees and students. These include chemical burns, fires and explosions, falling objects and people, cuts, dismemberment, electrocution, and death. In addition to risks created by instruction, the campus is subject to criminal activity, maintenance accidents, athletic and workplace injuries, and terrorist events.

Given the number of risks that exists, it is impossible to list, let alone address, all of them. Nevertheless, the campus has implemented a comprehensive safety program that employs monitoring, education and policies. To achieve a safe environment, it requires all employees and students to follow established policies and procedures, and to use common sense. The campus contracts with a 3<sup>rd</sup> party Security Department,

which has a Security Officer on duty 24/7. In addition, the Marshall Police Department is approximately 3 miles away and the Marshall Fire Station approximately 1 mile away.

## Objectives

The objectives of the audit were to ensure student and employee safety and security are being achieved on the Marshall campus, and that policies and procedures are in place to ensure on-going safety.

## Scope & Methodology

The scope of our audit included all safety related policies and procedures, physical characteristics of all buildings, instructional lab practices, police department practices, crime and fire reports, and emergency communication procedures. Given the size of the campus and the infinite number of safety risks that exists, this audit was not intended to verify all risks. It was intended to identify common ones that are known to exist on this campus and institutions of higher education in general.

To accomplish our objectives, we utilized a safety checklist developed by the Texas School Safety Center. It addressed common risks found on institutions of higher education. It was developed using numerous State and Federal resources. Our method of testing primarily consisted of observation, inquiry, and policy review. We also inquired about the handling of all sexual assaults reported on the 2014 Campus Crime report. [NOTE: None were reported in Marshall]

## General Observations

We observed numerous positive practices that help ensure a safe and secure campus. The following is a list of several of them:

- At least one Security Officer is on duty 24/7.
- Employees participate in First Aid/CPR training every 2 years.
- Fire extinguishers, fire alarms, periodic fire drills, first aid kits, and eye washes are deployed throughout the campus.
- 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.
- Comprehensive safety related policies are in place. Some of the more extensive ones include a Campus Disaster Plan, Emergency Evacuation of Buildings, Personal Protective

Equipment, Business Continuity Plan, Sexual Assault and Harassment Policies.

- The Annual Campus Fire & Safety Report is prepared and published. The report lists certain reported crimes and fires that occurred on the campus in the last calendar year.
- Material Safety Data Sheets of chemicals that are stored on campus are generally being maintained, as well as a Master MSDS list.
- Artificial defibrillator devices (AED's) are deployed in some buildings and management is considering purchasing additional AED's.

### Summary of Finding


We identified one area we feel warrants management's consideration. This is addressed in detail in a supplemental report.

### Opinion

Based on the audit work performed, the campus has implemented appropriate safety and security practices to ensure students and employees are reasonably safe. The issues cited in the finding are best characterized as enhancements to current procedures, and are not observations of neglect. In my opinion, the campus is not only safe, but has the appropriate procedures in place to ensure it remains that way.

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

Submitted by:

  
Jason D. Mallory, CPA, CIA

June 15, 2015

Date

---

***AUDIT FINDING DETAIL***

---

<p>Finding #1: We identified one area we feel warrants management's consideration. This is addressed in detail in a supplemental report.</p>
--

*To protect the safety of students and employees, our detailed observations and management's corrective action plans are detailed in a supplemental report that is considered confidential in accordance to Section 3.07, §551.076 of the Texas Government Code.*



**Internal Audit Department**

**Audit Report**

**Safety & Security Audit  
of  
TEXAS STATE TECHNICAL COLLEGE  
North Texas Campus**

**June 16, 2015**

**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

### Table of Contents

Executive Summary .....	1-2
Introduction.....	2
Objectives .....	3
Scope & Methodology .....	3
General Observations.....	3-4
Summary of Finding .....	4
Opinion .....	4
Audit Finding Detail.....	5

Internal Audit completed a comprehensive audit of safety and security policies and processes at the North Texas campus of TSTC as of May 31, 2015.

The purpose of the audit was to verify the existence of comprehensive policies and procedures that assist with protecting both students and employees.

Because of the numerous risks the campus faces, we utilized checklists developed by the Texas School Safety Center for use by community colleges. Community colleges are required by TEC 37.108(b) to conduct and report a safety audit every 3 years. While this regulation does not specifically apply to TSTC, the checklist is relevant.

We tested the following areas in this audit:

- Behavioral assessment/correction policies and procedures,
- Physical characteristics of all facilities (instructional and administrative) which affect safety/security,
- Fire/emergency responder related issues,
- Alarms and security cameras,
- Landscaping,
- Access controls to facilities,
- Police policies and procedures,
- Emergency Management/Business Continuity policies and procedures,
- Lab safety for students and employees,
- Transportation safety and related policies,
- Other general policies and procedures that have been implemented to achieve safety (sexual harassment/assault, timely warning, emergency closing, etc.), and
- Emergency communications processes.

We conducted observations in 2 instructional and administrative buildings.

Based on our audit work, we feel the campus has developed and put into place comprehensive and robust safety measures. Some examples include collaborating with the Red Oak ISD Police Department to provide security services, and the implementation of numerous safety related policies and procedures.

A more detailed list of our positive observations is located in the general observations section of this report.

Because of the number of procedures in this audit, we identified some areas that needed management's attention. Some of these observations were simply overlooked by management, so accordingly we made recommendations to address the minor deficiencies. For example, we observed an eye wash station/kit and fire blanket were not in one lab and some instances where evacuation routes and other safety related information were not posted in classrooms. These observations were isolated occurrences in individual buildings, can be easily remedied, and/or did not represent issues pervasive throughout the entire campus. We felt that these observations did not warrant being communicated in detail to the Board given their nature. We gave this list to the management team to address.

## Introduction

Campus safety and security is the single most important objective at any educational institution. Without adequate safety processes, all other objectives are put at risk.

TSTC's North Texas consists of 2 buildings, the Industrial Technology Center (ITC) and the Career & Technology Building (CATE). The ITC is a 100,000-plus sq. foot building that recently opened in September 2014 and offers 9 Programs. The CATE building is a 28,000 sq. foot building that is shared with Red Oak Junior High; TSTC's portion of the building is leased from Red Oak ISD.

Both buildings are located approximately half a mile from each other and located near of I-35 and approximately 20 miles from Dallas.

The technologies taught at TSTC pose inherent safety risks to both employees and students. These include fires and explosions, falling objects and people, cuts, dismemberment, electrocution, and death. In addition to risks created by instruction, the campus is subject to criminal activity, maintenance accidents, workplace injuries, and terrorist events.

Given the number of risks that exists, it is impossible to list, let alone address, all of them. Nevertheless, the campus has implemented a comprehensive safety program that employs monitoring, education and policies. To achieve a safe environment, it requires all employees and students to follow established policies and procedures, and to use common sense. To assist, the campuses have an agreement with the Red Oak ISD Police Department to provide security services. In addition, the Red Oak Police and Fire Departments are located approximately 3 miles away.

## Objectives

The objectives of the audit were to ensure student and employee safety and security are being achieved on the North Texas campus, and that policies and procedures are in place to ensure on-going safety.

## Scope & Methodology

The scope of our audit included all safety related policies and procedures, physical characteristics of all buildings, instructional lab practices, police department practices, crime and fire reports, and emergency communication procedures. Given the infinite number of safety risks that exists, this audit was not intended to verify all risks, rather was intended to test common ones that are known to exist on this campus and institutions of higher education in general.

To accomplish our objectives, we utilized a safety checklist developed by the Texas School Safety Center. It addressed common risks found on institutions of higher education. It was developed using numerous State and Federal resources. Our method of testing primarily consisted of observation, inquiry, and policy review. We also inquired about the handling of any reported sexual assaults. [NOTE: None were reported in North Texas]

## General Observations

We observed numerous positive practices that help ensure a safe and secure campus. The following is a list of several of them:

- Security is provided by the Red Oak ISD Police Department; one officer is assigned to each building.
- There are security cameras installed, and monitored by Red Oak ISD Police Department.
- Safety training is facilitated by the Red Oak ISD Police Department. In addition, employees in the CATE building participate in evacuation and active shooter drills required by the ISD.
- Fire alarms and first aid kits are deployed throughout the campus. In addition, the CATE building has a nurse on-site.
- Employees at the CATE building have access to a radio utilized by the Red Oak ISD Police Department, notifying them immediately in case of emergencies.
- Comprehensive safety related policies are in place; currently, North Texas utilizes policies implemented at TSTC Marshall.
- Material Safety Data Sheets of chemicals that are stored on campus are generally being maintained.



- Artificial defibrillator devices (AED's) are deployed in the CATE building and management is considering purchasing additional AED's for the ITC building.

### Summary of Finding

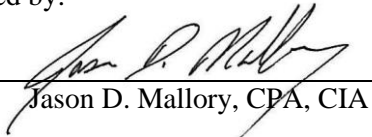
We identified one area we feel warrants management's consideration. This is detailed in a supplemental report.

### Opinion

Based on the audit work performed, the campus has implemented appropriate safety and security practices to ensure students and employees are reasonably safe. The issues cited in the finding are best characterized as enhancements to current procedures, and are not observations of neglect. In my opinion, the campus is not only safe, but has the appropriate procedures in place to ensure it remains that way.

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

Submitted by:



Jason D. Mallory, CPA, CIA

June 16, 2015

Date

---

***AUDIT FINDING DETAIL***

---

<p>Finding #1: We identified one area we feel warrants management's consideration. This is detailed in a supplemental report.</p>
---

*To protect the safety of students and employees, our detailed observations and management's corrective action plans are detailed in a supplemental report that is considered confidential in accordance to Section 3.07, §551.076 of the Texas Government Code.*



# External Penetration Testing Final Report



**For: Texas State Technical College**

**Version: 1.1**

**2 June 2015**

Issued by:  
MainNerve, LLC.  
5825 Mark Dabling Blvd, Ste 160  
Colorado Springs, CO 80920  
[www.mainnerve.com](http://www.mainnerve.com)

**CONFIDENTIAL**

---

## Origination

---

This report contains confidential information concerning Texas State Technical College (TSTC), as well as methods used by MainNerve for detecting and exploiting these vulnerabilities, if any. TSTC should take precautions to protect the confidentiality of the information contained herein.

MainNerve will retain a copy of the report for future reference. Any documents pertaining to this project will be stored in a secure area within the MainNerve offices in Colorado Springs, CO. While MainNerve is confident that security vulnerabilities of the target systems have been identified, there is no absolute assurance that a test of this nature will identify all possible security concerns. MainNerve used multiple vulnerability scanning tools and software to analyze and determine relevant findings.

The recommendations presented in this report are based on current technologies and known security threats as of the date of this engagement. As technology and risks evolve, vulnerabilities and mitigation recommendations associated with this project may also change. TSTC is encouraged to consult with MainNerve for clarification and assistance beyond this penetration test in understanding the context of this report.

MainNerve has prepared this report for TSTC. This document and any associated technical data will not be shared with other organizations or individuals without express written consent of TSTC.

---

## Executive Summary

---

Between April 13 and 22, 2015, MainNerve performed external vulnerability scans and penetration testing of TSTC external networks. The scope of the penetration test included a *white box*, or “limited knowledge”, test of all external devices identified by TSTC during the planning phase. The tools used for the penetration test consisted of a mix of publicly available tools downloaded from the Internet collectively with commercial and proprietary software. Both manual and automated testing methods were used to detect and/or validate the existence of exploitable vulnerabilities. For this project, MainNerve employed primarily manual techniques.

The objective of this penetration test was to compromise or otherwise gain access to TSTC’s network, effect unauthorized changes, and exploit resources using any means necessary, including attempting exploits and using “hacker” techniques. The scope of the test was presented in the Rules of Engagement (Attachment 1) approved by TSTC. It included:

- Network enumeration and asset identification (live host discovery)
- Service and network port identification
- Vulnerability assessment using commercial and open source vulnerability scanning software
- Attempts to penetrate TSTC’s network(s) by attacking external networks identified in the Rules of Engagement (Attachment 1)
- Penetration testing of the most critical vulnerabilities found, if any, in the TSTC-controlled production web-based applications
- Daily interim reports that provide technical updates to the TSTC designated staff

The detailed findings are included in the technical section of this report. It is also important to note that our assessment represents a point in time. Hence, this penetration test does not reflect zero-day exploits or other exploits not previously known. And while MainNerve is confident that the majority of vulnerabilities have been identified, there is no guarantee that all possible security exposures have been identified. TSTC should continue to regularly assess and/or audit its security posture.

---

## Summary of Results

The overall risk posed to Texas State Technical College as a result of this penetration test is Medium. This means that remote attacker has a limited degree of accessibility to the TSTC infrastructure that could be collected and potentially used to direct further attacks against TSTC users (see Table 1).

MainNerve performed passive and active scanning against all the address ranges provided by TSTC. Multiple findings were discovered, including Critical- and High-rated vulnerabilities. At no time, however, was TSTC's network security perimeter breached by MainNerve. That is, MainNerve did not gain access to the internal network by actively exploiting any vulnerabilities or misconfigurations.

MainNerve determined that TSTC maintains a prominent web presence as evidenced by the large number of web sites and/or web-accessible systems and applications. In one instance, MainNerve determined that a TSTC web site was vulnerable to a SQL injection attack. Upon approval from TSTC, MainNerve executed the SQL injection and subsequently retrieved student registration data, including full names, home addresses, email addresses, and telephone numbers. Other data of interest included TSTC staff-related information that contained contact information and work roles.

There are also many systems exposed to the Internet with services that could be accessed and enumerated easily using clear text protocols, such as SNMP. By exploiting this misconfiguration, MainNerve downloaded specific details regarding the target system. Most of the systems detected were printers whose value lay in the fact that the internal IP address was disclosed. This information allows an attacker to profile the internal network for potential future attacks. MainNerve also connected to several printers over TCP port 9100 and sent print commands.

MainNerve detected various Polycom telecom systems, some that are video enabled. Unauthenticated telnet sessions were permitted on one system wherein remote dialing over POTS (Plain Old Telephone System) call to a MainNerve facility was possible.

A host containing a critical vulnerability related to MS14-066 which could allow remote code execution by a remote user. MainNerve attempted to exploit this vulnerability on several occasions without success. To date, the vulnerability still remains on the host system.

A system containing critical vulnerabilities related to the Novell eDirectory software was detected on a different TSTC web site. MainNerve did not attempt to exploit this vulnerability due the extremely high risk of a denial of service condition should the exploitation fail. MainNerve estimates that the system is currently in service with the vulnerability still present.

#### Risk Rating Overview

MainNerve considers various factors when determining the final risk rating. This risk rating includes such factors as the threat vulnerability, potential attack scenario(s), and the impact of a successful exploitation/attack. A MainNerve analyzes the results and findings of the penetration test—independent of a vulnerability scan—and measures the severity of the vulnerability, the likelihood of exploitation, and the direct effect the attack may have on a client.

Level	Definitions
<b>Critical</b>	The client's network is directly vulnerable to a cyber attack. The client's network may have already been breached by an unknown third party. An attacker has privileged (root/administrative/system-level) access to the client's network. The impact to the client's network includes the loss or disclosure of sensitive data, corrupted data, and the interruption of primary network services. Losses will include non-compliance, if applicable, and violation of privacy.
<b>High</b>	The potential of a successful cyber attack is very likely. This is due to the presence of one or more critical vulnerabilities and the ease of exploitation. An attacker may gain user-level access to the network, but not privileged access. The impact to the client's network could involve the loss or disclosure of sensitive data. Losses may include non-compliance, if applicable, and violation of privacy.
<b>Medium</b>	An attack is possible, but not without some difficulty. Vulnerabilities, if exploited, may expose data that when assembled with other data, may represent a loss of confidentiality. Losses may include non-compliance, if applicable, and violation of privacy.
<b>Low</b>	An attacker cannot readily breach a client's network. Although vulnerabilities may be present, they are not easily exploitable and/or would not result in remote access. The impact to the client's network could involve the disclosure of data not sensitive in nature. Information disclosed could be used to identify personnel and leverage future attacks.

*Table 1 – MainNerve Penetration Test Risk Rating*

## MEMORANDUM

TO: Jason Mallory  
Audit Committee

FROM: Richard Martin, Director of Information Security

THROUGH: Rick Herrera, VC – Office of Information Technology

DATE: June 17, 2015

SUBJECT: MainNerve Penetration Test – Corrective Action Plan

---

An external penetration test was performed by MainNerve in May to test the security of TSTC's externally facing web presence. We welcomed your participation in this engagement to add a level of assurance that the results of the tests were unbiased. While the testing firm was not able to penetrate the network to obtain any regulatory protected data, they did find five areas that should be further secured.

The following is our intended courses of action for each area identified as needing enhancement.

### **SQL Injection**

The site [www.waco.tstc.edu](http://www.waco.tstc.edu) was found to be vulnerable to SQL injection. The code that allowed this was immediately isolated and removed. Our Information Security personnel validated the correction by attempting to repeat the injection without success. Additionally, on July 1<sup>st</sup> 2015 the Waco.tstc.edu site will be deactivated in favor of the single tstc.edu website. We consider this item resolved, however, MainNerve will verify our assertion in follow-up testing.

### **Network Printer Exploitation gained through the use of SNMP**

The ability to access select printers via the internet has never been an intended practice. We have eliminated the ability to access through the internet the specific printers identified by MainNerve. We are currently unaware of any printers with the same vulnerability, but will immediately eliminate the risks if they present themselves in the future. We consider this item resolved, however, MainNerve will verify our assertion in follow-up testing

### **Heartbleed Vulnerability**

MainNerve detected and successfully exploited the Heartbleed vulnerability on a video conference type device in Harlingen. We updated the software which allowed this vulnerability, and will continue to work with all vendors to ensure software/firmware is always up to date. We consider this item resolved, however, MainNerve will verify our assertion in follow-up testing



**Polycom Devices**

MainNerve was able to utilize default vendor credentials to access a video conferencing device, and were able to make phone calls from the device. We will remove the default credentials. This will also be verified in the upcoming MainNerve follow-up testing.

**SMTP Relay Attempts**

Four SMTP servers discovered by MainNerve send emails from limited internal devices and applications. Even though SMTP servers are publicly visible, and our security safeguards were able to restrict MainNerve from doing anything. We consider this issue properly controlled.

We appreciate the work performed by MainNerve because it has helped us improve our security. We look forward to the follow-up testing, and will keep you apprised of those results as well.



# TEXAS HIGHER EDUCATION COORDINATING BOARD

P.O. Box 12788 Austin, Texas 78711

Harold W. Hahn  
CHAIR

Robert W. Jenkins, Jr.  
VICE CHAIR

David D. Teuscher, M.D.  
SECRETARY OF THE BOARD

Gerald T. Korty  
STUDENT REPRESENTATIVE

Dora G. Alcalá  
Ambassador Sada Cumber  
Fred Farias, III  
Janelle Shepard  
John T. Steen, Jr.

Raymund A. Paredes  
COMMISSIONER  
OF HIGHER EDUCATION

512/ 427-6101  
Fax 512/ 427-6127

Web site:  
<http://www.thecb.state.tx.us>

June 25, 2015

Dr. Gisela Figueroa  
Texas State Technical College-Harlingen  
1902 North Loop 499  
Harlingen, TX 78550-3697

RE: AY 2014 A-133 Evaluation and Desk Review Management Letter

Dear Gisela Figueroa:

The Texas Higher Education Coordinating Board (THECB), as a federal pass-through entity, must provide due diligence to ensure its subrecipients meet the requirements of the Single Audit Act Amendments of 1996, as prescribed in OMB Circular A-133 Compliance Supplement and Government Auditing Standards.

The purpose of this letter is to issue our management decision regarding the fiscal review of your organization's Appropriation Year 2014 A-133 evaluation and desk review to communicate compliance issue(s), if any, on federal funds awarded to your institution by THECB.

**A-133 Audit Findings:** None

**Desk Review Findings:** THECB staff noted non-compliance issues in the following areas:

NONE

We greatly appreciate the cooperation and assistance provided by your staff during our review. If you have any questions or comments, please contact Gracie Lopez via email at [Gracie.Lopez@THECB.state.tx.us](mailto:Gracie.Lopez@THECB.state.tx.us) or call 512-427-6499.

Thank you for your assistance,

A handwritten signature in blue ink that reads "Mark Poehl".

*Mark Poehl, CPA, CIA, CISA, CFE*  
Director, Internal Audit & Compliance



**Texas State Technical College  
Internal Audit  
Attestation Disclosures**

Responsible Management	Issue Reported by Management	Report Date	Management's Corrective Action Plan	Internal Audit Assistance/Follow-up
	<b>No new issues were reported this quarter.</b>			

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.