

**TEXAS STATE TECHNICAL COLLEGE**

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

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

**Thursday, May 14, 2020**

**1:00 p.m.**

**AGENDA**

- I. MEETING CALLED TO ORDER BY AUDIT COMMITTEE CHAIR CURTIS CLEVELAND**
- II. COMMITTEE CHAIR COMMENTS**
- III. MINUTE ORDERS**  
  
None.
- IV. REPORTS:**

- 1. Status of Fiscal Year 2020 Audit Schedule & Other Projects ..... A-3  
*Jason D. Mallory*
- 2. Summary of Audit Reports..... A-7  
*Jason D. Mallory*
- 3. Follow-up Schedule & Status ..... A-11  
*Jason D. Mallory*

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

4. Internal Network Penetration Test - Waco (20-016A).....	A-19
<i>Jason D. Mallory</i>	
5. TAC 202 - Quarterly Update (20-010A).....	A-26
<i>Jason D. Mallory</i>	
6. Clery Act Compliance Audit (20-014A).....	A-28
<i>Jason D. Mallory</i>	
7. Attestation Disclosures.....	A-35
<i>Jason D. Mallory</i>	

**V. CHANCELLOR COMMENTS**

**VI. BOARD COMMENTS**

**VII. ADJOURN**

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

**Texas State Technical College**  
**Internal Audit**  
**Status of Fiscal Year 2020 Audit Schedule & Other Projects**



Description	Division/Campus	Status	Project No.	Report Date
<b>INTERNAL AUDITS</b>				
Public Funds Investment Act Compliance Audit	Finance	Complete	20-004A	9/26/19
Internal Network Penetration Test (EWCHec)	OIT/Safety & Security/Provost Office	Complete	20-002A	9/27/19
C4EO Audit - 2019 Audit	C4EO	Complete	19-032A	11/15/19
Benefits Proportionality Audit	Payroll	Complete	20-001A	12/6/19
Contract Audit - 2019 Audit	Finance	Complete	19-031A	12/12/19
Internal Network Penetration Test (Harlingen)	OIT, Harlingen Campus	Complete	20-011A	12/13/19
Internal Network Penetration Test	Waco Campus	Complete	20-016A	3/10/20
TAC 202 Follow-up Audit	OIT	In Progress	20-010A	10/7/2019, 1/9/20, 4/1/20
Clery Act Audit	Safety & Security	Complete	20-014A	4/8/20
Career Services Audit		In Progress		
Airport Operations Audit		In Progress		
Contract Compliance Audit		In Progress		
Help Desk Audit		In Progress		
Waco Bookstore Operational Audit		In Progress		
Harlingen Bookstore Operational Audit		In Progress		
Bookstore Point of Sale System - TAC 202 Audit		In Progress		
Field Support Audit				
Accounting Controls Audit				

**EXTERNAL AUDITS**

DOD: Voluntary Education Institutional Compliance Program 2019 – Corrected Feedback Report	VA Office	Complete		10/2/19
DPS: Texas N-Dex Audit Compliance Report	Waco Police	Complete		12/13/19
USDA: NIFA Audit of UTRGV Subaward of 2015-38422-24061(03)	OSP/Harlingen	Complete		No report issued
TWC Audit of Apprenticeship Training Program in Harlingen: This was an internal audit of TWC processes by their internal auditors.	OSP/Harlingen	Complete		No report issued
TWC: Monitoring review of SDF Contract # 2418SDF002	OSP/Harlingen	In Progress		
TWC: Monitoring review of SDF Contract # 2418SDF003	OSP/Harlingen	In Progress		
VA Audit	VA Office/Waco Campus	In Progress		
Texas Comptroller: Duplicate Payment Audit	Procurement	In Progress		
TWC: Desk Review of Contract 2918PEB000	TWC	In Progress		

Description	Division/Campus	Status	Project No.	Report Date
<b>OTHER INTERNAL PROJECTS</b>				
Face to Face Complaint: A concern was raised that a manager accepted impermissible gifts in exchange for awarding contracts. Results: Unable to determine whether gifts were accepted, but validated that a personal relationship existed between the manager and the vendor which created an appearance of impropriety and bias. As a result, the manager was separated from the College, and enhanced procedures were implemented to prevent recurrence.	Facilities	Complete	20-006I	10/8/19
Internal Hotline: Employee alleged hostile work environment. Results: Complaint was forwarded to HR for investigation/resolution.	HR Related Issue	Complete - No report issued by IA	20-017I	12/12/19
Internal Hotline: Allegation of conflict of interest due to related party purchases and violation purchasing regulations. Results: This same complaint was investigated in October 2017 at project 18-015I. We determined that the conflict was disclosed to the COI and Executive Management/Board, majority of purchases were paid by the Foundation, and the accused was not involved in the procurement process.	Procurement	Complete - Referred to previous investigation performed in FY 2018.	20-018I (18-015I)	10/31/17
Report by COI Committee: A concern was raised that an employee has indirectly benefitted by referring students to his/her part time employer, and disclosed personal information. Results: Determined that the employee is dually employed. Recommended he not be involved in the referral process going forward.	Harlingen/Counseling	Complete	20-019I	1/14/20
Request by management: A concern was raised that an employee(s) were involved in selling/purchasing surplus property outside of the prescribed process. Results: Determined that asset control procedures were lax. We could not validate the specific concern, but cited several examples of poor controls that needed to be addressed.	Central Receiving/Instruction (Harlingen Campus)	Complete	20-015I	1/17/20

Description	Division/Campus	Status	Project No.	Report Date
SAO Hotline: Former student at TSTI Amarillo alleged he is having to pay student loans that he never received in 1985. Results: Found no evidence to support allegation. Evidence indicated that his financial aid was suspended due to poor academic performance. And there was no indication that he had raised a concern before this complaint was filed, which is suspicious.	Financial Aid	Complete	20-021I	1/30/20
Employee Complaint: Allegation that a current pilot instructor used College assets for personal use. Results: Did not identify any intentional misuse, but identified opportunities for assets to be better controlled and safeguarded. The person was relieved of his management duties.	Instructional/Air Pilot Training	Complete	20-020I	3/2/20
SAO Hotline: A student claimed she was fraudulently registered for classes in Fall 2010. She was upset that her transcript was being withheld, with outstanding charges being sent to collections. Results: Determined that the student never paid for the classes, yet was not de-registered. She had appealed in the past, but the appeals were denied because an instructor noted her as attending. Attempts were made to contact the student, but the student never returned calls. To not impede her education, the College has released holds on her transcript, and will not pursue further collection efforts.	Registrars Office - Harlingen Campus	Complete	20-022I	3/10/20
Report on Maxient: Someone complained that donated funds were being misdirected, students were progressing inappropriately, and expired ingredients were being used in recipes. Results: Allegations had no merit, but determined fund raising activities and donations were not being directed through the Foundation as required by policy.	Instructional/Culinary Arts (Waco Campus)	Complete	20-024I	4/7/20

Description	Division/Campus	Status	Project No.	Report Date
SAO Hotline: Essentially, student complained that his lack of financial aid caused him to fail coursework. Results: Determined that this was a customer service matter, and forwarded to the Registrar's Office to contact former student. Student has yet to respond. IA did determine that the financial aid was withheld pending verification of a parent W-2. Student evidently does not understand the requirement, after repeated attempts were made by financial aid staff to resolve the matter.	North Texas Campus	Complete	20-023I	No report issued. Complaint was referred to Registrar's Office for resolution.
SAO Hotline: Employee complained that her supervisor is forcing her work more hours than she is being compensated for. Results: This was referred to HR for investigation and resolution. Pending response.	Recruiting	In Progress	20-028I	
Consulting: Serving on Workday implementation. Role is limited to monitoring re-designed business processes for unmitigated risks, and raising security concerns.	OIT/Finance/HR	In Progress		
Consulting: Serving on Waco Task Force for demolishing numerous buildings. Role is limited identifying potential risks and suggesting ways to mitigate those risks.	Facilities/Finance	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
Internal Network Penetration Test - Waco (20-016A)	1. Through scripted telephone calls in which our actual telephone number was masked, we were able to obtain the logon credentials of 5 employees to the College's ERP system. We were also able to access the Portal through an employee's unsecured laptop without detection, and found computers in one student computer lab could access the internal network	See finding.	1.1 The entire campus community will be reminded of the importance of never disclosing passwords to anyone. That communication will also address the need to challenge people in areas that they do not typically frequent, to lock doors to office when they are vacant for an extended period of time, and to lock computers when away from them.	Patti Tate	3/31/20
			1.2 Each of the 5 people who were compromised will be specifically counseled. For the person who was compromised for a second time, his actions will be discussed with his supervisor and will be reflected in his 2020 annual performance review. Any further instances will be escalated as appropriate, which may include loss of IT access and termination of employment.	Patti Tate	3/31/20

Report Name & No.	Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
			1.3 In regards to the student computer lab that was accessible to the internal network, this lab was scheduled to be placed on Active Directory in April 2020. Implementation was expedited, and the issue was resolved on March 2, 2020.	Scherwitz	3/2/20
2.	We noted physical security lapses.	We were able to access filing cabinets in an administrative office while the office was occupied, and identified a building with an open window after hours, and broken window latches.	See CAP 1.1. The windows in the administrative building were fixed.	Tate & Scherwitz	3/31/20

<b>TAC 202 - Quarterly Update (20-010A)</b>	1.	8 more controls were implemented between January 1, 2020, and March 31, 2020, for the systems we have audited to date.			
---	----	--	--	--	--

<b>Clery Act Compliance Audit (20-014A)</b>	1.	Some required policy statements were either missing or inaccurate in the 2019 AFSR, procedures related to Campus Security Authorities need to be improved, and we could not reconcile crime data submitted to the ED.	<ul style="list-style-type: none"> <li>- Some hate crime categories and statistics were omitted from the ASFR for all of the campuses.</li> <li>- For select campuses, some reported crimes were more than were recorded in the crime logs.</li> <li>- Some required policy statements were either incomplete or inaccurate.</li> </ul>	1.1 The next Annual Security Report will include all missing information, and all instances of inaccurate information in this report and information submitted to the Department of Education will be eliminated.	Torres	10/1/20
---	----	---	---	---	--------	---------



Report Name & No.	Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
		<p>-The list of CSAs in the ASFR was inaccurate.</p> <p>- Several recognized CSAs were not notified/reminded of their responsibilities, or documentation was not maintained.</p> <p>-Some crime and fire statistics reported directly to the ED via their web-based collection system could not be reconciled to the ASFR. Specifically, some of the statistics was less than was included in the ASFR.</p>	<p>1.2 Processes are being developed in coordination with SHEA Officers, HR, Student Development, Chiefs of Police, and Risk Management, to ensure all Campus Security Authorities are aware of their responsibilities by maintaining an accurate list of all such people and the training they have received. Standardized processes are also being developed by the Chiefs of Police. Compliance will be verified through reviews of the requirements during the preparation of the Annual Security Report, and through frequent communication and input from all areas previously listed.</p>	Torres	10/1/20
	2. Emergency notification procedures and evacuation drills need to be enhanced.	<p>We determined the ENS is not being tested once every term, as required by policy and as stated in the ASFR. Furthermore, some students were not included to receive notifications, even though they did not opt out. These appeared to be half-time students.</p>	<p>2.1 Effective immediately, the ENS will be tested at least once each term by Strategic Communications. They will coordinate with the Risk Management to identify and resolve any issues associated with employees and students not receiving ENS notifications.</p>	Torres	Immediately
		<p>We also determined fire evacuation drills were not conducted at several buildings throughout the College in calendar year 2018, as stated in the 2019 ASFR. The Safety Department was in a period of transition during that time, which probably explains the lapse.</p>	<p>2.2 Since 2018, the Risk Management has implemented fire drills on each campus with assistance from its increased staff of SHEA Officers. Those drills are tracked and reviewed by the Director of Risk Management.</p>	Torres	Immediately

Report Name & No.	Audit Finding	Summary of Finding Support	Management's CAP(s)	Resp. Sr Mgr	Expect. Complete Date
USDA: NIFA Audit of UTRGV Subaward of 2015-38422-24061(03)		No findings identified.			
TWC Audit of Apprenticeship Training Program in Harlingen		No findings identified.			

Texas State Technical College  
Internal Audit  
Follow Up Schedule & Status



Completion Summary			
	12/31/19	3/31/20	Cleared from (Added to) Schedule
Audits from FY 2017 & Earlier	2	2	0
Audits from FY 2018	1	1	0
Audits from FY 2019	10	8	2
Audits from FY 2020	0	2	(2)
<b>Net Total</b>	13	13	0
Findings from FY 2017 & Earlier	2	2	0
Findings from FY 2018	1	1	0
Findings from FY 2019	11	9	2
Findings from FY 2020	0	4	(4)
<b>Net Total</b>	14	16	(2)

**Highlights:**

TAC 202 Audits: 8 more controls were implemented.
PCI Audit (18-009A) has 8 controls pending Internal Audit review.
Graduation Audit (19-008A): All outstanding items cleared.
Helicopter Investigation (19-019I): Billing exceptions are pending review by Internal Audit.
Contracting Audit (19-032A): all items cleared.

Report Name & No., Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
Summary of Departmental Audits (Marshall Welding Department 17-013A, Fort Bend Diesel 17-023A, Fort Bend HVAC 17-022A), Hoekstra	1. We identified numerous exceptions related to inventory control in the Welding Department.	1.1 Summary : Create a cross-divisional team and review existing policies and procedures related to the inventory process.	<b>Substantially Complete:</b> Determined in follow-up testing performed in November 2018 and June 2019 that all but one deficiency was corrected. The remaining deficiency related to asset transfers will be retested in FY 2020.		8/31/20
TAC §202 Compliance Audits (17-002A) (19-004A), (19-003A), (19-017A), Herrera	1. Several required controls were not yet implemented.	As noted in the report, a majority of the required controls have been implemented with the remaining controls being evaluated and addressed. For the controls not yet implemented, we are evaluating the associated risk to TSTC and associated applicability in our environment to prioritize implementation. IT Security along with TAC 202 compliance is a priority for TSTC.	<b>Ongoing:</b> At 3/31/20, 6 systems and the IT general controls have been audited. A total of 12 general controls and 78 (total for all systems audited) application controls were not yet implemented. In this quarter, 8 controls were improved to implemented status.		Ongoing

Report Name & No., Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
PCI Compliance Audit (18-009A), Herrera	1. Numerous IT related controls and/or their control elements, as prescribed by PCI DSS, have not been implemented. As such, PCI DSS compliance is not being fully met.	1.1 In an effort to ensure the protection of payment card data for students and employees, The Office of Information Technology has been working with Food Services to resolve a number of important control deficiencies during the audit and will continue to review and implement recommendations moving forward. As we anticipate that the review and implementation review of 100 controls across 6 objectives will take over a year, we will prioritize controls that have the largest impact on the protection of cardholder data. As part of this process, we will also implement the recommendation of an annual assessment of PCI-DSS controls to ensure ongoing adherence to PCI-DSS compliance changes.	<b>Ongoing:</b> As of 1/9/19, PCI controls were being mapped to TAC 202 controls so implementation efforts will be optimized. At 7/12/19, 8 controls were pending Internal Audit's review.		Ongoing

Report Name & No., Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
Helicopter Training Program Investigation (19-0091), Kilgore, Hoekstra, Herrera	1. Summary: We did not identify any training of flight students performed by a contractor. Additionally, the student composition of HPTP when combined with the fixed wing enrollment figures complies with the VA's 85/15 rule. While we made several observations indicating the program was ineffectively managed in the past, current management appears to be taking steps to improve the operation of the program to make it more efficient and less costly. We did, however, identify accounting processes and controls that need to be improved to ensure the correct flight fees are charged to students, and any unused Chapter 33 funds are returned timely to the VA.	Various tasks - See investigative report. Summary: all observations for improvement will be addressed	<b>Pending Review</b>		Immediately

Workplace Harassment Audit (19-014A), Hoekstra, Mayfield	1. Current policies and procedures related to workplace harassment can be improved by implementing several of the recommendations offered by the EEOC in their 2016 report.	1.1 A single, comprehensive policy will be created that includes all 10 of the EEOC's recommended elements.	<b>Ongoing:</b> On 3/27/20 has begun revising existing policies.		9/30/19
		1.2 Frequent reminders to the employees on the College's expectations, with some of those reminders coming directly from the Executive Team.	<b>Ongoing:</b> Followed up on 3/27/20. No response received yet.		9/30/19
		1.3 A single comprehensive policy will be created, with various forms of training being conducted.	<b>Ongoing:</b> Followed up on 3/27/20. No response received yet.		10/31/19

Report Name & No., Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
Departmental Audit - Challenger Centers (19-018A & 19-019A), Mayfield, Balli, Wooten	1. Risks associated with minors on campus would be better managed by performing enhanced background checks on CLC employees, and requiring them to attend periodic training.	1.1 Determine whether DPS Fingerprint service can be utilized, and if not identify the an entity that will best serve this need.	<b>Ongoing:</b> 3/27/20: Per Angela Sill, the College's finger print background checks does not include staff positions. HR has offered to start performing standard background checks on these employees annually. However, this practice has not yet started.		10/31/19
	2. Accounting processes for revenue need to be improved.	2.1 Accounting processes will be changed to record deferred/unearned revenue when missions are scheduled and invoiced.	<b>Pending Review:</b> 4/6/20: Email to accounting inquiring about this corrective action. Waiting on response from Accounting Dept.		11/30/19
		2.2 Validate revenue and accounts receivable monthly.	<b>Pending Review:</b> 4/6/20: Email to accounting inquiring about this corrective action. Waiting on response from Accounting Dept.		11/30/19
<b>Admissions Process Audit (19-017A), Stuart-Carruthers, Foshie, Arredondo</b>	1. Application processes need to be improved to ensure documentation is standardized, and communications with applicants are timely.	1.1 Enrollment Services 2.0 was created to reduce such errors and during the audit period trainings were taking place on new processes. All Enrollment Coaches will be issued their own stamps for documents. A Conditional Enrollment Agreement went into effect in July 2019 whereas prior to 2.0 a form was not required by all campuses.	<b>Ongoing:</b> CAPs not due yet.		5/31/20

Report Name & No., Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
		1.2 With the implementation of ES 2.0, a shift in communications moved from Colleague to Salesforce. While automatic letters still generate from Colleague, those tracks are under review to ensure communication is timely. A communication committee has been developed that will manage the creation, editing, and scheduling of all communication to applicants. Phone numbers have been updated as needed.	<b>Ongoing:</b> CAPs not due yet.		5/31/20
	2. Access to admissions and enrollment related mnemonics in Colleague needs to be better restricted.	2.1 Submitted a request to OIT to evaluate access for employees in question and remove if not appropriate. The Executive Registrar will collaborate with Human Resource and OIT to identify a process to ensure access is evaluated by the appropriate department when changes in employment within the college occur.	<b>Ongoing:</b> CAPs not due yet.		6/30/20
<b>Internal Network Penetration Test - Waco (20-016A), Scherwitz, Tate</b>	1. Through scripted telephone calls in which our actual telephone number was masked, we were able to obtain the logon credentials of 5 employees to the College's ERP system. We were also able to access the Portal through an employee's unsecured laptop without detection, and found computers in one student computer lab could access the internal network.	1.1 The entire campus community will be reminded of the importance of never disclosing passwords to anyone. That communication will also address the need to challenge people in areas that they do not typically frequent, to lock doors to office when they are vacant for an extended period of time, and to lock computers when away from them.	<b>Pending Review</b>		3/31/20



Report Name & No., Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
		1.2 Each of the 5 people who were compromised will be specifically counseled. For the person who was compromised for a second time, his actions will be discussed with his supervisor and will be reflected in his 2020 annual performance review. Any further instances will be escalated as appropriate, which may include loss of IT access and termination of employment.	<b>Pending Review</b>		3/31/20
		1.3 In regards to the student computer lab that was accessible to the internal network, this lab was scheduled to be placed on Active Directory in April 2020. Implementation was expedited, and the issue was resolved on March 2, 2020.	<b>Pending Review</b>		3/2/20
	2. We noted physical security lapses.	See CAP 1.1. The windows in the administrative building were fixed.	<b>Pending Review</b>		3/31/20
<b>Clery Act Compliance Audit (20- 014A), Torres</b>	1. Some required policy statements were either missing or inaccurate in the 2019 AFSR, procedures related to Campus Security Authorities need to be improved, and we could not reconcile crime data submitted to the ED.	1.1 The next Annual Security Report will include all missing information, and all instances of inaccurate information in this report and information submitted to the Department of Education will be eliminated.	<b>Ongoing</b>		10/1/20

Report Name & No., Resp. Sr Mgr	Internal Audit Finding	Management's CAP(s)	Internal Audit Comments on Status	Management Comments on Status	Expect. Complete Date
		1.2 Processes are being developed in coordination with SHEA Officers, HR, Student Development, Chiefs of Police, and Risk Management, to ensure all Campus Security Authorities are aware of their responsibilities by maintaining an accurate list of all such people and the training they have received. Standardized processes are also being developed by the Chiefs of Police. Compliance will be verified through reviews of the requirements during the preparation of the Annual Security Report, and through frequent communication and input from all areas previously listed.	Ongoing		10/1/20
	2. Emergency notification procedures and evacuation drills need to be enhanced.	2.1 Effective immediately, the ENS will be tested at least once each term by Strategic Communications. They will coordinate with the Risk Management to identify and resolve any issues associated with employees and students not receiving ENS notifications.	Pending Review		Immediately
		2.2 Since 2018, the Risk Management has implemented fire drills on each campus with assistance from its increased staff of SHEA Officers. Those drills are tracked and reviewed by the Director of Risk Management.	Pending Review		Immediately

**Internal Audit Department**

**Audit Report**

**Internal Network Penetration Test Audit (20-016A)**  
**TEXAS STATE TECHNICAL COLLEGE**  
**Waco Campus**

**March 10, 2020**

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

## **Executive Summary**

Between December 10, 2019 and January 20, 2020, we performed vulnerability scans and penetration testing of the College's internal network on the Waco Campus.

The primary objective of this project was to ensure sensitive information stored and processed by primary systems, and systems directly supporting the confidentiality, integrity, and accessibility of those systems, have controls in place to detect and prevent attacks from unauthorized individuals on the campuses. Physical and logical security controls, to include the actions and habits of personnel, were targeted in this project. We specifically focused on likely attack vectors that could be exploited by bad actors to gain unauthorized access to sensitive information and information technology assets.

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

In general, sensitive information and resources were reasonably protected. However, we were able to secure user credentials to Colleague through our telephone calls, and were able to access a user's laptop while he stepped away from his office. We also noted lapses in physical security presented us with opportunities to access sensitive information or other College assets.

## **Introduction**

Information and asset security requires a coordinated effort from all employees. Sensitive information is stored in both physical and electronic formats. Information and assets in the physical form are protected through physical controls, such as locks on doors, restricted access to rooms, cameras, and the presence of alert employees. Information in the electronic form are similarly protected to the same controls, but also rely upon the use of unique logon credentials to systems, data encryption, network segregation, and other various IT security policies procedures.

The Office of Information Technology (OIT) Division assist the College with its operational needs by maintaining secure IT networks, providing end-user support and training, assisting with IT

purchases, and maintaining critical databases and offering critical application support. They are also critical in designing and implementing IT related controls. Every employee in the College has a responsibility, though, to protect information and assets.

The Waco Campus houses the main data center for the College. All critical in house servers are located on the Waco Campus, and backed to up to the Harlingen Campus for redundancy. In FY 2015, an external test was performed which simulated attacks from off-campus sites through the internet by a consultant. This tested on-campus attacks by exploiting risks identified through first hand observations and research through resources available to anyone. In FY 2017, an internal test similar to the one performed in this report was conducted.

To ensure the integrity of the results of this test, we only notified the Provost prior to our tests in an attempt to achieve reliable results. This test verified not only physical and logical controls related to safety and security and IT security, it also validated human behavior in certain regards.

## **Objectives**

The objectives of the internal network penetration test were to:

- Ensure primary systems, and systems directly supporting the confidentiality, integrity, and accessibility of primary systems have controls in place to detect and prevent attacks.
- Ensure unauthorized individuals on campus are unable to access privileged systems, sensitive data, or other College assets (equipment, computers, etc.)
- Verify the effectiveness of end-user training on threats related to information security and asset security.
- Allow the College to gain insight into real-world attack vectors that may have not been previously considered or tested.

This test was not intended to verify all risks the Campus faces during an actual attack. We focused on likely scenarios based upon the information we gathered during our testing.

## **Scope & Methodology**

The scope of the penetration test included the physical and logical securities of core network equipment, access network equipment, and servers located on the Waco Campus. It also included employee awareness and vigilance against potential related attacks that compromise IT systems and sensitive data. The following industry standards served as our methodology:

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

## General Observations

Most employees demonstrated an awareness with regard to who was visiting certain areas of buildings/common areas, and were vigilant in protecting sensitive information. Wired and wireless networks are segregated between privileged and guest accounts, with services being appropriate on each. Wireless access points are unlikely to emit signals that can be used by bad actors outside of the physical perimeters of the originating building. Access to closets and rooms containing critical networking equipment were kept locked during and after business hours. Access to faculty offices were kept restricted from unauthorized users by locking doors during business hours. Most computer lab desktops were restricted through the use Active Directory Naming Services, requiring any user to have a web advisor username and password in order for them to be used. Finally, most buildings were inaccessible after business hours, unused ports were inactive, and sensitive information was not found during “dumpster diving” attempts and casual observations of staff desks and workspaces.

## Summary of Findings

1. Through scripted telephone calls in which our actual telephone number was masked, we were able to obtain the logon credentials of 5 employees to the College’s ERP system. We were also able to access the Portal through an employee’s unsecured laptop without detection, and found computers in one student computer lab could access the internal network.
2. We noted physical security lapses.

## Opinion

Based on the audit work performed, IT assets and information are generally well protected on the Waco Campus. But the deficiencies cited in this audit indicate certain employees need enhanced training.

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

---

Jason D. Mallory, CPA, CIA

---

March 10, 2020

Date

---

## **AUDIT FINDING DETAIL**

---

Finding #1: Through scripted telephone calls in which our actual telephone number was masked, we were able to obtain the logon credentials of 5 employees to the College's ERP system. We were also able to access the Portal through an employee's unsecured laptop without detection, and found computers in one student computer lab could access the internal network.

**Criterion:** We identified employee telephone numbers and email addresses through a review of information located on the internet. Using that information, we sent phishing emails and made vishing telephone calls to a sample of employee. The purpose of those attempts were to solicit logon credentials to the Portal and/or Colleague.

We also walked the campus posing as a student. We attempted to go in areas that should have been restricted, like the data center, get on employee computers in offices that were open and vacant, and get on computers in student computer labs.

5 employees provided their Colleague logon credentials during telephone calls we made. This system allows access to sensitive information. We also intentionally targeted some of the users from our last test. Unfortunately, 1 of the 5 employees was also compromised during our last test. He was counseled during the last test, and warned that he would be tested again in the future.

We were able to access the Portal through an employee's computer in his vacant office. The employee's machine was not password protected, and the Portal credentials automatically filled. No one detected us.

Finally, we found one student computer lab that was still open to the public without having to enter logon credentials. We determined that the internal network was accessible through this lab.

**Consequences:** Exposure of sensitive student and employee information and increased risk of inappropriate activity on the College's network.

**Possible Solution:** We recommend all campus employees be informed of our project results, and everyone be reminded of their responsibilities to protect sensitive information and IT assets. We further recommend that the 5 individuals that actually provided their credentials and the one whose computer we accessed be specifically counseled so that they can learn and improve their actions.

For the computer lab, we recommend credentials be required to access the machines by any user, and access to the internal network be eliminated.

### Management Response

The Office of the Provost (Waco) agrees with the observations and recommendations made in the audit regarding the need to re-educate people on the importance of protecting information and resources. The 5 instances in which employees disclosed their user logon credentials appear to be the result of lapses in judgement, and their failure to adhere to the directives to never disclose passwords to anyone. The majority of the employees who were tested evidently passed, which suggests training efforts are more often successful. By March 31, 2020, the entire campus community will be reminded of the importance of never disclosing passwords to anyone. That communication will also address the need to challenge people in areas that they do not typically frequent, to lock doors to office when they are vacant for an extended period of time, and to lock computers when away from them. Furthermore, each of the 5 people who were compromised will be specifically counseled. For the person who was compromised for a second time, his actions will be discussed with his supervisor and will be reflected in his 2020 annual performance review. Any further instances will be escalated as appropriate, which may include loss of IT access and termination of employment. Patti Tate, Waco Provost, will be responsible for implementing these corrective actions.

The Office of Information Technology agrees with the observations and recommendations made in the audit regarding the need to re-educate people on the importance of protecting information and resources, and agrees with the actions previously stated by the Provost. In regards to the student computer lab that was accessible to the internal network, this lab was scheduled to be placed on Active Directory in April 2020. Implementation was expedited, and the issue was resolved on March 2, 2020. Shelli Scherwitz, Executive Director/OIT, will be responsible for ensuring the corrective actions have been implemented.



---

## AUDIT FINDING DETAIL

---

Finding #2: We noted physical security lapses.

**Criterion:** We attempted to access physical areas, such as the data center and IT related closets, that should have been restricted. We did not limit ourselves to just those areas, though, because ever building contains assets and potentially sensitive information. Our attempts were conducted during business hours while employees were present, and after business hours when most facilities should have been locked.

The majority of attempts to access areas without being challenged or prevented by a physical control such as locks were thwarted. However, we were able to access one administrative area with employees present during business hours, and access their filing cabinets. Not until we were leaving did anyone challenge us.

Also found an open window to another administrative building after business hours. Upon further inspection, we noted that more windows in that same building do not lock, so the easily facility is accessible at any time.

**Consequences:** Exposure of sensitive student and employee information and increased risk of theft of assets.

**Possible Solution:** We recommend the employees in the buildings with the noted deficiencies be counseled on their responsibilities to protect assets to challenge unknown people in areas they would not normally be, and to ensure all doors and other entrance points are secured after hours. We also recommend a work order be immediately submitted for the windows that will not lock.

### Management Response

The Office of the Provost (Waco) agrees with the observations and recommendations made in the audit regarding the need to re-educate people on the importance of protecting information and resources. Please refer to the corrective actions outlined in Finding #1. Patti Tate, Waco Provost, will be responsible for implementing these corrective actions.

The Office of Information Technology agrees with the observations and recommendations made in the audit regarding the need to re-educate people on the importance of protecting information and resources, and agrees with the actions previously stated by the Provost. The physical plant was contacted to fix windows in the administrative building that did not lock. That issue was immediately corrected after Internal Audit disclosed their test results. Shelli Scherwitz, Executive Director/OIT, took responsibility for ensuring the corrective actions were implemented.



To: Audit Committee  
 From: Jason D. Mallory, Audit Director  
 Subject: TAC 202 Compliance – Quarterly Update  
 Date: April 1, 2020

The purpose of this memo is to provide you the current implementation statuses of IT controls required by TAC 202 tested in numerous internal conducted since 2017. Each quarter we test select controls which were previously found to be not implemented. Annually, the list of systems will increase as we continue to audit. From January 1 through March 31, 2020, **8** more required controls were implemented.

## RESULTS

### General Controls

Original Audit: June 28, 2017

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted <sup>Note 1</sup>	Total
Jan 2020 – Mar 2020	53	19	12	2	86
Oct 2019 – Dec 2019	53	19	12	2	86
Change	0	0	0	0	

*Note 1: Management has elected to not implement controls SC-20 & SC-21 because implementing is too costly, and does not provide additional risk mitigation. Furthermore, they have researched other agencies and institutions of higher education, and no one else has implemented the controls.*

### Colleague

Original Audit: June 28, 2017

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
Jan 2020 – Mar 2020	33	11	5	0	49
Oct 2019 – Dec 2019	33	11	5	0	49
Change	0	0	0	0	

### Perceptive Content

Original Audit: June 28, 2017

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
Jan 2020 – Mar 2020	23	14	12	0	49
Oct 2019 – Dec 2019	23	13	13	0	49
Difference	0	+1	-1	0	

**Maxient**

Original Audit: February 25, 2019

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
Jan 2020 – Mar 2020	30	3	16	0	49
Oct 2019 – Dec 2019	29	2	18	0	49
Difference	+1	+1	-2	0	

**Google Suite**

Original Audit: December 10, 2018

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
Jan 2020 – Mar 2020	33	7	9	0	49
Oct 2019 – Dec 2019	33	5	11	0	49
Difference	0	+2	-2	0	

**Target X**

Original Audit: September 30, 2019

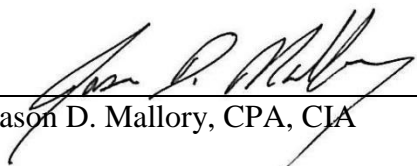
Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
Jan 2020 – Mar 2020	25	1	23	0	49
Oct 2019 – Dec 2019	23	0	26	0	49
Difference	+2	+1	-3	0	

**Informatica Server**

Original Audit: September 30, 2019

Period	Implemented	Implemented with Recommendations	Not Implemented	Risk Accepted	Total
Jan 2020 – Mar 2020	36	0	13	0	49
Oct 2019 – Dec 2019	36	0	13	0	49
Difference	0	0	0	0	

Submitted by:



Jason D. Mallory, CPA, CIA

April 1, 2020

Date

cc: Mike Reeser, Chancellor/CEO  
 Ricardo Herrera, VC/CSSO  
 Shelly Scherwitz, Executive Vice President/OIT



## **Internal Audit Department**

### **Audit Report**

**Jeanne Clery Disclosure of Campus Security Policy and Campus Crime  
Statistics Act - Compliance Audit (20-014A)**

**TEXAS STATE TECHNICAL COLLEGE**

**April 8, 2020**

**This audit was conducted in accordance with the**

***International Standards for the Professional Practice of Internal Auditing***

**of the Institute of Internal Auditors.**

## **Executive Summary**

We recently completed an audit of the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act of 1998, more commonly referred to as the Clery Act (Clery). The audit focused on the procedures currently in place to ensure safety and compliance with Clery, to include information contained in the most recent Annual Security & Fire Safety Report (ASFR) published in October 2019. Crime data submitted to the Department of Education was also reviewed in this audit.

The primary objective of the audit was to ensure processes are in place to achieve the key requirements of Clery, and to verify the most recent ASFR was accurate and included all necessary disclosures. In addition to reviewing the 2019 ASFR, we also reviewed the 2019 Campus Safety & Security Survey submitted to the Department of Education, relevant crime & fire logs, the emergency notification system (Everbridge) and related processes, and the Building Evacuation Report and Evaluation Checklist.

Our testing revealed the College generally has procedures in place to achieve compliance. An AFSR is published by October 1 of each year, and made available to the campus community. It includes crime and fire statistics, and most of the required policy statements are accurate. There is a coordinated effort on the part of each campus to compile relevant information, with the majority of the data being verifiable.

We found instances, though, where compliance either was not achieved, or procedures need to be enhanced. The details of these findings are noted in the Audit Finding Detail section of this report.

## **Introduction**

In 1990, Congress enacted the Crime Awareness and Campus Security Act of 1990 (Title II of Public Law 101-542), which amended the Higher Education Act of 1965 (HEA). This act required all postsecondary institutions participating in HEA's Title IV student financial assistance programs to disclose campus crime statistics and security information. The act was amended in 1992, 1998, 2000 and 2008. The 1998 amendments renamed the law the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act in memory of a student who was slain in her dorm room in 1986. It is generally referred to as the Clery Act and is in section 485(f) of the HEA. All higher educational institutions that receive Title IV funds must comply with Clery.

An overview of the basic compliance requirements of Clery follows:

- Emergency notification and evacuation procedures must be implemented. This program must notify the campus community of emergency situations so that appropriate actions can be taken to help ensure individual's safety.
- Crime prevention and awareness programs and campaigns must be in place for the campus community.

- An Annual Security and Fire Safety Report (ASFR) must be published by October 1 of each year that reports specific crime and fire data for the preceding 3 calendar years. That same report must include specific policy statements related to crime and fire reporting, crime and fire prevention, and statements regarding safety and emergency situations.
- Campuses with either police departments or security departments must maintain daily crime and fire logs that include specific elements. The logs must be readily available for inspection by the public upon request.
- Persons throughout each campus must be appointed to serve as campus security authorities. These same individuals must collect and report alleged Clery crimes so that they can be included in the ASFR.
- Criminal statistics must be requested from external law enforcement agencies, and annual crime and fire statistics must be submitted electronically to the U.S. Department of Education (ED).
- Procedures must be in place to handle disciplinary actions related to dating violence, domestic violence, sexual assault and stalking.
- A missing student notification procedure must be in place.

The campus Police Departments compile the ASFR, and submit crime information to the ED. The ASFR is prepared in cooperation with local law enforcement agencies, and employees throughout the College to include housing, enrollment management, and anyone appointed as a campus security authority.

The Chiefs of Police lead most compliance efforts, with individual campus efforts being overseen by the 3 Chiefs. All report to the Commissioner of Safety and Security.

### **Objectives**

The objectives of the audit were to determine whether key Clery requirements were met as of November 30, 2019, and to verify the 2019 ASFR information is accurate and complete. These objectives included determining the accuracy and timeliness of reports, the sufficiency of records retention, the correctness of security policies described in the ASFR, and the accessibility of the related information

### **Scope & Methodology**

The scope of our audit included the 2019 Annual Security & Fire Safety Report (ASFR) which includes crime and fire statistics for calendar years 2016, 2017, and 2018. And included related procedures that were in place as of November 30, 2019. The 2016 Edition of the Handbook for Campus Safety and Security Reporting published by the Department of Education (Handbook) served as the basis for our testing. We utilized the “Checklist for Campus Security Safety and Security Compliance” in appendix C of the Handbook, and security related Statewide Operating Standards.

### **General Observations**

The College published and distributed the most recent ASFR by October 1. In addition, the crime and fire statistics were submitted to the Department of Education (ED) via the Web-based data collection within the required timeframe. The College has written emergency response and evacuation procedures in place, and a robust process to alert the campus community in emergency situations. Crime and fire logs were readily available for inspection. Numerous departments, to include campus Police, Housing, Human Resources (HR), Strategic Communications, and others coordinate efforts. Finally, the Police and other employees provided professional and prompt assistance during the course of this audit.

### **Summary of Findings**

1. Some required policy statements were either missing or inaccurate in the 2019 AFSR, procedures related to Campus Security Authorities need to be improved, and we could not reconcile crime data submitted to the ED.
2. Emergency notification procedures and evacuation drills need to be enhanced.

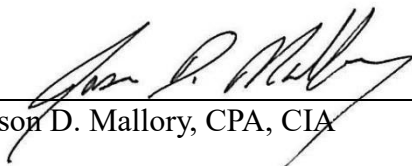
### **Opinion**

Based on the audit work performed, the College has procedures in place to generally comply with the Clery Act, and the 2019 Annual Security & Fire Report was materially complete and accurate. Nevertheless, we identified areas that require improvement before full compliance is achieved.

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

---

April 8, 2020

Date

---

### *AUDIT FINDING DETAIL*

---

Finding #1: Some required policy statements were either missing or inaccurate in the 2019 AFSR, procedures related to Campus Security Authorities need to be improved, and we could not reconcile crime data submitted to the ED.
---

**Criterion:** We attempted to verify the accuracy and timeliness the 2019 ASFR & electronic crime and fire data submitted to the ED, the accuracy and completeness of policy statements included in the ASFR, records retention requirements, and the accessibility of the information.

The following reports and documentation were tested in this audit:

- 2019 Annual Security & Fire Safety Report (ASFR)
- 2019 Campus Safety & Security Survey submitted to the Department of Education
- Crime Logs
- Fire Logs
- The emergency notification system (Everbridge) notification report.
- Building Evacuation Report and Evaluation Checklist

We noted the following compliance deficiencies that need to be addressed:

#### ASFR

- Some hate crime categories and statistics were omitted from the ASFR for all of the campuses.
- For select campuses, some reported crimes were more than were recorded in the crime logs.
- The following required policy statements were either incomplete or inaccurate:
  - A statement was missing to inform the reader that some external law enforcement agencies did not provide crime statistics or responded to requests, even though they were requested to do so.
  - Definitions for crimes related to the domestic & dating violence and stalking differed from the definition in the 2016 Handbook for Campus Safety & Security Reporting published by the ED.
  - The policy related to missing students excluded some required information.
  - The reported number of fire drills was incorrect.
  - The fire statistics did not include the street address for each student housing facility.
  - There was no statement regarding future plans, or lack thereof, to enhance fire safety.
  - The statement related to emergency response and evacuation did not include all required information.



### Campus Security Authorities (CSAs)

- The list of CSAs in the ASFR was inaccurate. We found some people listed that had not been employees for several years.
- Several recognized CSAs were not notified/reminded of their responsibilities, increasing the risk that all reportable incidences were not disclosed.
- Evidence that several CSAs were notified/reminded of their responsibilities was not maintained. As such, we have no assurance that these people were actually notified.

### Web-based Data Collection to the ED

- Some crime and fire statistics reported directly to the ED via their web-based collection system could not be reconciled to the ASFR. Specifically, some of the statistics was less than was included in the ASFR.

**Consequences:** Potential fines levied by the ED from up to \$35,000 to \$58,328 per violation effective January 14, 2020. More significantly, egregious non-compliance could result in the inability to offer Federal Financial Aid.

**Possible Solution:** Internal Audit recommends utilizing Appendix C Checklist for Campus Safety and Security Compliance each year as a self-audit to ensure all required information is included in the ASFR. We also recommend regularly updating the list of CSAs, and ensuring those people are made aware of their responsibilities and documentation be maintained of those efforts. Finally, we recommend all information submitted to the ED be accurate.

### **Management Response**

The Office of Safety & Security agrees that certain policy statements were missing from the 2019 Annual Security Report, processes related to Campus Security authorities need to be improved, and information submitted to the Department of Education was incomplete. These observations were the result of numerous issues including leadership and organizational changes within the Office of Risk Management. By October 1, 2020, the next Annual Security Report will include all missing information, and all instances of inaccurate information in this report and information submitted to the Department of Education will be eliminated. Furthermore, processes are being developed in coordination with SHEA Officers, HR, Student Development, Chiefs of Police, and Risk Management, to ensure all Campus Security Authorities are aware of their responsibilities by maintaining an accurate list of all such people and the training they have received. Standardized processes are also being developed by the Chiefs of Police. Compliance will be verified through reviews of the requirements during the preparation of the Annual Security Report, and through frequent communication and input from all areas previously listed. Aurelio Torres, Commissioner of Safety will be responsible for ensuring implementation of these corrective action plans. More detailed corrective actions were provided to Internal Audit to assist with their follow-up review.

---

### **AUDIT FINDING DETAIL**

---

**Finding #2:** Emergency notification procedures and evacuation drills need to be enhanced.

**Criterion:** We reviewed the emergency notification system (ENS) used to rapidly notify the campus community of emergency situations. We also reviewed fire drill information to ensure drills are conducted as frequently as stated in the ASFR.

We determined the ENS is not being tested once every term, as required by policy and as stated in the ASFR. Furthermore, some students were not included to receive notifications, even though they did not opt out. These appeared to be half-time students.

We also determined fire evacuation drills were not conducted at several buildings throughout the College in calendar year 2018, as stated in the 2019 ASFR. The Safety Department was in a period of transition during that time, which probably explains the lapse.

**Consequences:** Increased risk of students/employees being exposed to unsafe conditions without being directed how to respond.

**Possible Solution:** Internal Audit recommends all fire drills and tests of the ENS be performed according to College policy, and as stated in the ASFR. We also recommend the all current students and employees be included in the ENS, unless they specifically opt out of notifications.

### **Management Response**

The Office of Safety & Security agrees that emergency notification system (ENS) has not been tested as frequently as required, and that certain people are not receiving notifications. We also agree that fire evacuation drills were not performed in the past in the frequency stated in the 2019 Annual Security Report. These deficiencies were primarily due to changes in leadership in Strategic Communications and the Office of Risk Management. Effective immediately, the ENS will be tested at least once each term by Strategic Communications. They will coordinate with the Risk Management to identify and resolve any issues associated with employees and students not receiving ENS notifications. Since 2018, the Risk Management has implemented fire drills on each campus with assistance from its increased staff of SHEA Officers. Those drills are tracked and reviewed by the Director of Risk Management. Aurelio Torres, Commissioner of Safety will be responsible for ensuring implementation of these corrective action plans. More detailed corrective actions were provided to Internal Audit to assist with their follow-up review.

Texas State Technical College  
Internal Audit  
Attestation Disclosures



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

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