Lisa R. Collier, CPA, CFE, CIDA
First Assistant State Auditor

An Audit Report on

Financial Processes at Texas State Technical College

April 2021

Report No. 21-017

An Audit Report on

Financial Processes at Texas State Technical College

SAO Report No. 21-017
April 2021

Overall Conclusion

Texas State Technical College (College) should strengthen its processes to ensure that it accounts for and disposes of its assets in accordance with Office of the Comptroller of Public Accounts (Comptroller's Office) requirements and College policy. Additionally, the College should strengthen certain controls over its financial system to ensure the reliability of its data. However, the College had processes to ensure that it made payments in accordance with applicable requirements.

Background Information

Founded in 1965, Texas State Technical College (College) serves Texas through its 10 campus locations:

- Abilene.
- Breckenridge.
- Brownwood.
- East Williamson County.
- Fort Bend County.
- Harlingen.
- Marshall.
- North Texas.
- Sweetwater.
- Waco.

The College is governed by a nine-member Board of Regents who are appointed by the governor to six year terms.

Source: Texas State Technical College.

Assets. The College did not have adequate controls over its assets and related document retention. Specifically, the College had weaknesses in its processes for the inventory of its assets, the reporting of accurate and complete asset data to the Comptroller's Office, and the disposition of assets.

Expenditures. The College had processes that ensured it paid vendors and made payments for travel-related and procurement card expenses in accordance with applicable requirements. The College also had policies in place that were sufficient to comply with certain requirements.

Information Technology. The College should strengthen its information technology (IT) controls to address significant security risks that could affect the reliability and security of data used for reporting financial information.

Table 1 on the next page presents a summary of the findings in this report and the related issue ratings. (See Appendix 2 for more information about the issue rating classifications and descriptions.)

This audit was conducted in accordance with Texas Government Code, Sections 321.0131 and 321.0132.

For more information regarding this report, please contact Cesar Saldivar, Audit Manager, or Lisa Collier, First Assistant State Auditor, at (512) 936-9500.

Table 1

Summary of Chapters and Related Issue Ratings		
Chapter	**Title**	**Issue Rating [a]**
1	The College Had Weaknesses in Its Asset Recording and Disposal Processes	Priority
2	The College Had Voucher Payment Policies and Procedures in Place to Ensure That It Complied With Applicable Requirements	Low
3	The College Should Strengthen Its Access Controls and Maintenance Processes to Help Ensure the Reliability of Its Financial Data	High

[a] A chapter is rated **Priority** if the issues identified present risks or effects that if not addressed could critically affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is required to address the noted concern and reduce risks to the audited entity.

A chapter is rated **High** if the issues identified present risks or effects that if not addressed could substantially affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern and reduce risks to the audited entity.

A chapter is rated **Medium** if the issues identified present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Action is needed to address the noted concern and reduce risks to a more desirable level.

A chapter is rated **Low** if the audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks or effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

Auditors communicated other, less significant issues separately in writing to College management.

Summary of Management's Response

At the end of Chapters 1 and 3 in this report, auditors made recommendations to address the issues identified during this audit. The College agreed with the recommendations in this report.

Audit Objectives and Scope

The objective of this audit was to determine whether Texas State Technical College has processes and related controls to help ensure it administers financial transactions in accordance with applicable requirements.

The scope of this audit included vendor payments, procurement card payments, travel payments, and asset disposals from September 1, 2018, through August 31, 2020. The scope also included a review of significant internal control components related to the College's financial processes.

Contents

Detailed Results

Appendices

Detailed Results

Chapter 1

The College Had Weaknesses in Its Asset Recording and Disposal Processes

Chapter 1 Rating:

Priority [1]

The College's processes were not adequate to ensure that (1) assets were inventoried in compliance with Office of the Comptroller of Public Accounts (Comptroller's Office) requirements, (2) all disposed assets were recorded and accurate in the State Property Accounting system (SPA), and (3) assets were disposed of in compliance with Comptroller's Office requirements or College policy. Additionally, the College's existing process did not ensure that it maintained support for all disposed assets.

As of September 2020, the College recorded 25,730 active assets in SPA with acquisition costs totaling $445,722,438. From September 1, 2018, through August 31, 2020, the College recorded 3,829 assets as disposed. Auditors selected a random sample of 25 disposed assets and the entire population of 22 assets reported as stolen for testing.

Asset Inventory

The College's inventory verification processes was not adequate to ensure that all assets were identified and accounted for. Specifically:

- **Donated assets.** The College's process was not adequate to ensure that donated assets were added to its inventory and SPA. When assets are received by the College, the assets are required by the College's policies and procedures to be tagged and recorded in SPA. The College's process, which is not documented, gives Central Receiving primary responsibility for the initial recording, tagging, and distribution of assets to the appropriate custodian. However, donated equipment is sometimes received directly by the departments rather than Central Receiving. The College's process relies on the receiving department notifying Central Receiving or the asset being identified during annual inventory. During testing, auditors noted that an asset stolen from the College had been donated directly to a department. This asset was not tagged or reported as received to Central Receiving through multiple annual inventories; therefore, when the asset was reported missing by an employee, the College did not have the item on its asset inventory list.

[1] The risk related to the issues discussed in Chapter 1 is rated as Priority because they present risks or effects that if not addressed could critically affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is essential to address the noted concern and reduce risks to the audited entity.

- **Auctioned assets.** Additionally, the College's process was not adequate to ensure that it accounted for auctioned assets. One tested asset was initially reported to law enforcement as missing after an employee left the College. Upon investigation, the police report indicated that the investigating officer determined that the asset had been auctioned without documenting the inventory or serial number. The police report was dated November 2017, while the College asserted that the asset had been auctioned more than six months earlier. According to the College, Central Receiving had not updated the College's asset management system when it received the asset or when the asset was auctioned. While the College was able to provide a receipt for the auction, auditors were not able to determine if it was the same asset reported as missing.

Requiring that all assets, including donated items, are inventoried and entered into SPA when received could help ensure that each asset is identified, accounted for, and recorded by the College in accordance with Comptroller's Office requirements.

Asset Disposals

Auditors analyzed the disposed assets reported in the College's financial system and SPA from September 1, 2018, through August 31, 2020, and determined that the College did not ensure that all disposed assets were reported in SPA. According to the College, it does not perform a reconciliation between its financial record system and SPA for all assets. As a result, a total of 101 disposed assets were not reported to SPA as required. Auditors included those assets with the assets reported in SPA and identified a population of 3,829 assets the College disposed from September 1, 2018, through August 31, 2020.

In addition, the College did not always maintain supporting documentation, dispose of assets, and notify law enforcement in accordance with Comptroller's Office rules. Specifically:

- The College did not consistently ensure that support required for the specific asset disposals was maintained. As a result, compliance with applicable rules could not be determined for 7 (28 percent) of 25 disposed assets tested because they were missing documentation to support the method of disposal. Additionally, for 4 (18 percent) of the 22 stolen assets tested, the investigation forms required by the Comptroller's Office for missing or stolen assets could not be located. Maintaining the investigation forms as required documents that an investigation was conducted and a determination was made whether the asset being stolen was the result of employee negligence.

- The College did not consistently ensure that it recorded the final disposition of assets in SPA in accordance with Comptroller's Office requirements. Specifically, the final dispositions of 3 (12 percent) of 25 assets tested were not recorded in SPA 2 calendar years from the date the asset went missing. For example, the College deleted a missing asset from SPA at the end of the second fiscal year after the asset was reported as missing, rather than two calendar years from the date reported missing, as required by the Comptroller's Office. Supporting documentation showed that a disposed asset tested was recorded as missing in SPA on March 21, 2018. The asset should have been disposed of after the conclusion of an investigation and no later than March 21, 2020, using the missing date recorded in SPA. However, the final disposal in SPA occurred on August 31, 2020.

- For 3 (14 percent) of 22 assets reported as stolen, law enforcement was not notified within 48 hours of the College determining that the assets had been stolen, as required by the College and the Comptroller's Office. In this instance, an employee received 15 donated computers, which were kept next to the employee's desk for reimaging. Two weeks later, the employee noticed 3 of the computers were missing; however, these assets were reported to law enforcement over 2 months after they were identified as stolen. Not reporting stolen assets to law enforcement in a timely manner could hinder the investigation and potential recovery of the assets.

Employee Negligence

The College did not consistently determine employee negligence when investigating stolen assets. The Comptroller's Office and the College require that an employee entrusted with property exercises, at a minimum, reasonable care for its safekeeping. Reasonable care means that steps have been taken to ensure:

- Acceptable upkeep and maintenance of the asset.

- Security of the asset.

- Ability to locate the asset at all times.

- Retention of documentation specifying the person responsible for the asset.

The determination of employee negligence when an asset is stolen is made by the employee's supervisor. Upon determination that the employee was negligent, the supervisor decides if the employee is required to reimburse the College. This leads to inconsistency, because the College does not have

procedures for determining negligence and responsibility for reimbursement. For example, during testing auditors identified 2 (9 percent) of 22 assets, a tablet computer and a self-defense device, that were reported stolen due to employee negligence, but only one employee was required to reimburse the College.

Additionally, 7 (32 percent) of 22 assets tested had been stolen after being left unattended in employee vehicles. Only one of those assets was determined by the College to have been stolen due to employee negligence, and as previously noted, this employee was not required to reimburse the College.

Having a documented process for the determination of employee negligence and responsibility for reimbursement could help ensure the determination is made consistently.

Recommendations

To strengthen its processes for tracking and disposing of assets, the College should:

- Develop and implement policies and procedures with detailed steps for asset management, including:
  - Performing asset disposals and recording asset disposals in SPA.
  - Maintaining accurate asset disposal information in SPA.
  - Maintaining appropriate documentation for disposed assets.
  - Reporting stolen assets to law enforcement within 48 hours.
  - Consistently determining employee negligence and whether an employee exercised reasonable care of stolen assets.
  - Reconciling its financial system of record with SPA for all assets.
- Revise its asset inventory process to ensure all assets, including donated items, are inventoried.

Management's Response

Management of Texas State Technical College (TSTC) agrees with the observations made in the audit. Weaknesses in asset recording and disposal processes are the result of system limitations and manual practices, which have been ongoing discussions and concerns at TSTC for several years. While TSTC has improved control over assets and their recordation, deficiencies recognized in the past were primary considerations when the College decided in fiscal year 2020 to replace Colleague with Workday. A comprehensive implementation process is currently underway, with asset control being a significant part of that project. TSTC expects the Finance portion of Workday (which includes asset management functionality) to be implemented in early calendar year 2022.

While Workday is still being implemented, we are taking the following actions to address the risks cited in this audit:

- *TSTC will not report to SPA after August 31, 2021, and as a result, there will be nothing to reconcile after we discontinue use.*

- *Donated assets have been recognized in the past as tripping points because they did not always go through a central office for approval and recordation. The specific issue cited in this audit is one example of the realized risks if the College is not informed of such donations. In recent years, an expectation has been communicated to all employees that all donations must be approved and accepted only by the Foundation. That group then ensures recordation. TSTC will continue to rely upon periodic communication to raise awareness of required procedures related to donated assets, but will also work to implement a comprehensive, annual fixed asset training for all employees by 12/31/2021, that addresses donated assets, as well as other asset management topics.*

- *The College has an approved disposal process in which all disposals are required to run through a centralized office. All disposals are made through an approved auction vendor, or transferred to another campus or state agency. The issue cited in the audit appears to most likely be related to delays in updating Colleague, which has been a noted concern in the past because of how cumbersome such updates are with Colleague. We feel the implementation of Workday will improve the timeliness and accuracy of tracking all assets, as well as the documentation maintenance. As noted earlier, by 12/31/2021, a comprehensive, annual asset management training will be conducted which will include communication of guidelines on processing documentation related to*

asset disposals, as well as processes for notifications to law enforcement and others related to missing, lost or stolen assets.

- *Concerning the determination of employee negligence, by August 31, 2021, a committee comprised of select individuals from asset accounting, inventory control and other operational divisions will be formed to review cases and make recommendations on lost or stolen assets. Using uniform criteria, the committee will consider the evidence and circumstances of each case to recommend to the supervising manager a proposed course of action ranging from "no action recommended", to recommendations for reimbursement and/or disciplinary measures due to employee negligence. In the event the recommendation is not followed by the manager, the committee will notify the respective Vice Chancellor for final consideration of the case.*

The Vice President of Procurement Services and Associate Vice Chancellor of Finance will be responsible for ensuring and validating these actions are implemented.

Chapter 2

The College Had Voucher Payment Policies and Procedures in Place to Ensure That It Complied With Applicable Requirements

Chapter 2 Rating:

Low [2]

The College established procedures to ensure that it paid vouchers in compliance with applicable rules, obtained appropriate approvals, made allowable purchases, and generally recorded expenditures accurately.

Additionally, the College had documented policies and procedures in place that were adequate to ensure compliance with applicable standards related to purchasing authority.

From September 1, 2018, through August 31, 2020, the College paid vouchers totaling $162,083,300. Auditors tested 103 vouchers that totaled $1,430,186 from three types of purchases: (1) 36 vendor payments totaling $1,074,942; (2) 35 travel purchases totaling $145,216; and (3) 32 procurement card purchases totaling $210,028. These transactions were:

- Supported by source documentation.
- Appropriately categorized.
- Approved by College staff according to its policies.
- Allowable.

Additionally, the College's policies and procedures complied with the standards of Texas Education Code, Section 51.9337, which require establishing a code of ethics, a contract management handbook, contract delegation guidelines, training for officers and employees involved in the contracting process, policies and procedures governing conflicts of interest, and internal audit protocols.

[2] The risk related to the issues discussed in Chapter 2 is rated as Low because the audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks or effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

Chapter 3

The College Should Strengthen Its Access Controls and Maintenance Processes to Help Ensure the Reliability of Its Financial Data

Chapter 3 Rating:

High [3]

The College should strengthen its information technology (IT) controls to address significant security risks that could affect the reliability and security of data used for reporting financial information.

Passwords

Auditors identified certain weaknesses related to application password settings and lock-out duration. To minimize security risks, auditors communicated details about these issues directly to the College's management in writing.

User Access

While the College had processes in place to complete periodic reviews of user access to its IT resources, as required by Title 1, Texas Administrative Code, Section 202.72, those processes were not adequate to ensure compliance with that statute. As a result, access to the College's financial system was not restricted to appropriate personnel, and some users had inappropriate access. Specifically, three former employees did not have their access removed upon leaving employment at the College. Those former employees had not been employed by the College for 13 to 20 months. Additionally, 10 employees had inappropriate levels of access that in some cases would allow them to initiate all of the steps of the payment process, including check printing. However, the College had appropriately restricted access to the Uniform Statewide Accounting System. Specifically, only current College employees had active accounts, administrative roles were restricted to appropriate personnel, and duties were appropriately segregated.

Implementing effective user access controls helps to ensure that access to critical information systems is appropriately restricted to minimize the risk of unauthorized changes to data.

Change Management

The College had a change management process in place to help ensure that changes to its financial system and the data within the system were appropriately tested, approved, and documented. However, the controls in

[3] The risk related to the issues discussed in Chapter 3 is rated as High because they present risks or effects that if not addressed could substantially affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern and reduce risks to the audited entity.

that process were not sufficient to provide reasonable assurance that changes to the College's financial system were properly implemented, as required by the Department of Information Resources' (DIR) *Security Control Standards Catalog* and the College's policies. Auditors tested 15 custom changes and 10 vendor patch changes and determined that changes were not consistently documented, tested, validated, approved, and implemented in compliance with College policy and DIR requirements. Additionally, the College's processes did not ensure that supporting documentation was consistently maintained, as required by the College policy and DIR. As a result, auditors were not able to determine if some custom application changes were migrated by someone other than the developer and whether changes were tested prior to implementation.

Specifically, out of 15 custom changes and 10 vendor patch changes tested:

- Five (33 percent) of the custom changes and 5 (50 percent) of the vendor patch changes did not have supporting documentation to indicate that they were tested and validated prior to implementation.
- Three (30 percent) of the vendor patch changes were put into production without supporting documentation to indicate the date of the change, the nature of the change, and the change's success or failure.
- None of the custom changes and vendor patch changes had supporting documentation to indicate approval prior to being put into production.
- Eleven (73 percent) of the custom changes and 3 (30 percent) of the vendor patch changes did not have supporting documentation to indicate that the changes were implemented by someone other than the developer.

Implementing appropriate change management controls would help enforce compliance with the change management process and help ensure that changes to information resources do not alter data or promote weaknesses that could affect data.

IT Policies and Procedures

The College's information systems security policies and procedures addressed significant IT functions, including password requirements, user access, and change management. However, the policies and procedures related to password requirements were not always consistent with DIR's *Security Control Standards Catalog* as required by Title 1, Texas Administrative Code, Chapter 202.

For example, the College's IT security policies did not establish the number of failed log-in attempts that may take place before an account is locked out and did not establish the minimum lock-out duration. DIR's *Security Control Standards Catalog* requirement of a maximum of 10 failed log-in attempts and a minimum lock-out duration of 15 minutes was required to be implemented by February 2017.

Recommendations

The College should review and update its IT security policies to ensure compliance with the requirements in Title 1, Texas Administrative Code, Chapter 202, and DIR's *Security Control Standards Catalog*. Specifically, the College should:

- Strengthen password length and account lock-out duration controls.
- Strengthen reviews of user access for its financial system.
- Assign user access rights appropriately based on users' job responsibilities, including reviewing and updating those rights when employees change positions or leave the College.
- Implement a segregation of duties to ensure that (1) changes to its IT systems comply with its change management policy and (2) user access rights are appropriately restricted.
- Maintain supporting documentation for changes to its IT systems, in accordance with its change management policy.
- Strengthen procedures to ensure that changes to its IT system are tested, validated, and appropriately approved before implementation, in accordance with its change management policy.

Management's Response

Management of Texas State Technical College agrees that control and maintenance processes within Colleague need to be improved to better ensure the integrity and reliability of the College's financial data. The control failures cited in this audit were primary considerations when the College decided to replace Colleague with Workday in fiscal year 2020. A comprehensive implementation process is currently underway, with access and security being key parts of that project. We expect the financial related portion of Workday to be implemented in early calendar 2022.

In the interim, we are taking the following actions to address the risks related to Colleague.

- *The College will strengthen password length and lock-out duration controls to address the issues communicated in writing.*
- *Regarding access:*
    - *When someone terminates employment, IT is notified by HR through the clearing process. To sign on to Colleague, the 3 users cited in this audit would have to have access to the internal network or the VPN. The 3 former employees cited in this audit did not have access to either, therefore, access to Colleague was unlikely. Nevertheless, we recognize the need to remove access in a more timely manner to all resources to further reduce the risk of inappropriate access. By May 1st, 2021, current user credentials in Colleague will be compared to a current employee list, with all exceptions being immediately corrected.*
    - *Conflicting access has been an ongoing challenge with Colleague because of the manner in which the system assigns access. Workday will make assigning and managing access easier to eliminate such issues. By May 1st, 2021, the specific access issues cited in this audit will be corrected.*
- *For programmatic changes to Colleague, to include security patches, there is a documented change management process that is expected. Effective immediately, any change to Colleague, will be documented, tested in the test environment, and properly approved prior to being rolled into production. This same process will be in place for Workday. To ensure compliance, IT Compliance will select a sample every month of changes and verify the established change management process has been implemented.*

The Executive Vice President of OIT and Executive Director of OIT Compliance will be responsible for ensuring and validating these actions are implemented.

Appendices

Appendix 1

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether Texas State Technical College has processes and related controls to help ensure it administers financial transactions in accordance with applicable requirements.

Scope

The scope of this audit included vendor payments, procurement card payments, travel payments, and asset disposals from September 1, 2018, through August 31, 2020. The scope also included a review of significant internal control components related to the College's financial processes. (see Appendix 3 for more information about internal control components).

Methodology

The audit methodology included reviewing relevant criteria; interviewing College staff; testing and analyzing vendor payments, travel expense reports, procurement card purchases, and asset disposals. In addition, auditors performed a review of selected general and application controls over the College's accounting and asset management systems.

Data Reliability and Completeness

To assess the reliability of the data sets extracted from the College's financial system of record, Colleague, as they related to vendor payments, travel expenditures, and procurement card purchases, auditors (1) observed the College staff extract the data sets, (2) reviewed queries, and (3) analyzed the data sets and queries for reasonableness and completeness.

To assess the reliability of the data sets downloaded from Citi Bank, auditors observed College staff download the data sets and reconciled them with the procurement card data extracted from the College's system of record.

To assess the reliability of the data sets extracted from the College's IT ticketing system as they relate to custom changes, auditors reviewed the report filters and the resulting output.

Auditors determined that those data sets were sufficiently reliable for the purposes of this audit.

Auditors also assessed the reliability of vendor patch changes that the College tracked using a spreadsheet but were unable to determine the completeness of the changes. However, this was the only list of the changes available; therefore, auditors used the data for sampling.

To assess the reliability of the data sets extracted from the State Property Accounting system (SPA) as they related to the disposed assets, auditors (1) reconciled the data to the College's Colleague system, (2) compared the data to the College's Annual Financial Report, and (3) analyzed the data sets for reasonableness and completeness. Based on that reconciliation, auditors determined that the data set extracted from SPA was not complete. However, the missing data was identified in the Colleague data set, and after combining the two data sets, auditors determined that they were sufficiently reliable for the purposes of this audit.

Sampling Methodology

To assess the College's asset disposal process and the change management of the College's financial system, auditors selected stratified nonstatistical samples of 25 disposed assets and custom and vendor patch changes through random selection. This sample design was chosen so the sample could be evaluated in the context of the population. Those test results may be projected to the population, but the accuracy of the projection cannot be measured.

Auditors selected nonstatistical samples of expenditures, primarily through random selection, from 3 categories:

1) 36 vendor payments totaling $1,074,942 from a population of 29,718 vouchers.

2) 32 travel payments totaling $210,029 from a population of 7,310 vouchers.

3) 35 procurement card payments totaling $145,216 from a population of 47,782 statement transactions.

In some cases, auditors selected additional items for testing based on risk. The sample designs were chosen to address specific risk factors identified in the population, such as dollar amount and procurement type. This sample design was chosen to ensure that the sample included a cross section of transactions. The test results as reported do not identify whether items were randomly selected or selected using professional judgment; therefore, it would not be appropriate to project the test results to the population.

Information collected and reviewed included the following:

- Statutes, rules, guidelines, and operating procedures relevant to vendor payments, procurement card purchases, travel expenditures, and asset disposals.
- Property transfer/deletion forms, stolen property investigation forms, and documentation to support asset disposal method.
- Payment vouchers, purchase orders, invoices, contract agreements, receiving documents, receipts, monthly procurement card statements, and expense reports.
- Expenditure data from the College's financial system of record, Colleague.
- The College's asset disposal data from SPA and Colleague.

Procedures and tests conducted included the following:

- Interviewed College management and staff.
- Analyzed data pertaining to vendor payments, procurement card purchases, travel expenses, and assets.
- Tested disposed assets for compliance with the Office of the Comptroller of Public Accounts (Comptroller's Office) requirements and College policy.
- Tested vendor payments, procurement card purchases, and travel expenses for compliance with College policies, rules, and applicable statutes.
- Tested selected general controls for Colleague and the Uniform Statewide Accounting System. Auditors also performed limited application control testing on Colleague.

Criteria used included the following:

- Texas Education Code, Section 51.9337.
- Title 1, Texas Administrative Code, Chapter 202.
- Comptroller's Office's *SPA Process User's Guide*.
- The College's travel card application and agreements.

- The College's standard operating procedures for its system of record (Colleague), asset disposals, real and personal property accounting, procurement card purchases, and travel expenditures.
- The Department of Information Resources' *Security Control Standards Catalog, Version 1.3*.

Project Information

Audit fieldwork was conducted from June 2020 through March 2021. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The following members of the State Auditor's staff performed the audit:

- Link Wilson (Project Manager)
- Jacqueline M. Thompson, CFE (Assistant Project Manager)
- Cody Bogan, CFE
- Evan Cresap, CPA
- Ashlie Garcia, MS, CFE
- Matthew J. Montgomery
- Mary Ann Wise, CPA, CFE (Quality Control Reviewer)
- Cesar Saldivar, CFE, CGAP (Audit Manager)

Appendix 2

Issue Rating Classifications and Descriptions

Auditors used professional judgment and rated the audit findings identified in this report. Those issue ratings are summarized in the report chapters/sub-chapters. The issue ratings were determined based on the degree of risk or effect of the findings in relation to the audit objective(s).

In determining the ratings of audit findings, auditors considered factors such as financial impact; potential failure to meet program/function objectives; noncompliance with state statute(s), rules, regulations, and other requirements or criteria; and the inadequacy of the design and/or operating effectiveness of internal controls. In addition, evidence of potential fraud, waste, or abuse; significant control environment issues; and little to no corrective action for issues previously identified could increase the ratings for audit findings. Auditors also identified and considered other factors when appropriate.

Table 2 provides a description of the issue ratings presented in this report.

Table 2

Summary of Issue Ratings	
Issue Rating	**Description of Rating**
Low	The audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks or effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.
Medium	Issues identified present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer program(s)/function(s) audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.
High	Issues identified present risks or effects that if not addressed could substantially affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern(s) and reduce risks to the audited entity.
Priority	Issues identified present risks or effects that if not addressed could critically affect the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is required to address the noted concern(s) and reduce risks to the audited entity.

Appendix 3

Internal Control Components

Internal control is a process used by management to help an entity achieve its objectives. Government Auditing Standards require auditors to assess internal control when internal control is significant to the audit objectives. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) established a framework for 5 integrated components and 17 principles of internal control, which are listed in Table 3.

Table 3

Internal Control Components and Principles		
Component	**Component Description**	**Principles**
Control Environment	The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.	▪ The organization demonstrates a commitment to integrity and ethical values. ▪ The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. ▪ Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. ▪ The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. ▪ The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Risk Assessment	Risk assessment is the entity's identification and analysis of risks relevant to achievement of its objectives, forming a basis for determining how the risks should be managed.	▪ The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. ▪ The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. ▪ The organization considers the potential for fraud in assessing risks to the achievement of objectives. ▪ The organization identifies and assesses changes that could significantly impact the system of internal control.
Control Activities	Control activities are the policies and procedures that help ensure that management's directives are carried out.	▪ The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. ▪ The organization selects and develops general control activities over technology to support the achievement of objectives. ▪ The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.
Information and Communication	Information and communication are the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.	▪ The organization obtains or generates and uses relevant, quality information to support the functioning of internal control. ▪ The organization internally communicates information, including objectives and responsibilities

Internal Control Components and Principles		
Component	**Component Description**	**Principles**
		for internal control, necessary to support the functioning of internal control. ▪ The organization communicates with external parties regarding matters affecting the functioning of internal control.
Monitoring Activities	Monitoring is a process that assesses the quality of internal control performance over time.	▪ The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. ▪ The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Source: Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, May 2013.

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable Dan Patrick, Lieutenant Governor, Joint Chair
The Honorable Dade Phelan, Speaker of the House, Joint Chair
The Honorable Jane Nelson, Senate Finance Committee
The Honorable Robert Nichols, Member, Texas Senate
The Honorable Greg Bonnen, House Appropriations Committee
The Honorable Morgan Meyer, House Ways and Means Committee

Office of the Governor

The Honorable Greg Abbott, Governor

Texas State Technical College

Members of the Texas State Technical College Board of Regents

- Mr. John K. Hatchel, Chair
- Mr. Tony Abad
- Mr. Curtis Cleveland
- Mr. Keith Honey
- Mr. Charles “Pat” McDonald
- Mr. Alejandro “Alex” Meade III
- Ms. Kathy Stewart
- Ms. Tiffany Tremont
- Mr. Ron Widup

Mr. Michael Reeser, Chancellor and CEO