

Meeting of the Board of Regents

Audit Committee Meeting

May 16, 2019

Waco, Texas



TEXAS STATE TECHNICAL COLLEGE

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

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

Thursday, May 16, 2019

10:30a.m.

AGENDA

- I. MEETING CALLED TO ORDER BY AUDIT COMMITTEE CHAIR IVAN ANDARZA**
- II. COMMITTEE CHAIR COMMENTS**
- III. MINUTE ORDERS**

None.

IV. REPORTS:

- 1. Status of Fiscal Year 2019 Audit Schedule & Other Projects A-3
Jason D. Mallory
- 2. Summary of Audit Reports A-5
Jason D. Mallory
- 3. Follow-up Schedule & Status A-10
Jason D. Mallory
- 4. Internal Network Penetration Test – North Texas (19-011A) A-21
Jason D. Mallory
- 5. Audit of the Maxient Application (19-003A) A-27
Jason D. Mallory
- 6. Internal Network Penetration Test – Ft. Bend (19-015A) A-33
Jason D. Mallory
- 7. Graduation Process Audit (19-008A) A-40
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 the preceding meetings. The estimated times are approximate and may be adjusted as required with no prior notice.

| | |
|--|------|
| 8. TAC 202 Compliance – Quarterly Update (19-012A) | A-47 |
| <i>Jason D. Mallory</i> | |
| 9. Audit of Police Evidence Room – Waco Campus (19-013A)..... | A-49 |
| <i>Jason D. Mallory</i> | |
| 10. Single Audit – FY 2018 Financial Statements & Federal Compliance | A-52 |
| <i>BKD</i> | |
| 11. Federal Portion of the Statewide Audit Report for the Year Ended August 31, 2018 | |
| | A-62 |
| <i>State Auditor's Office</i> | |
| 12. Attestation Disclosures | A-63 |
| <i>Jason D. Mallory</i> | |

V. CHANCELLOR COMMENTS

VI. BOARD COMMENTS

VII. ADJOURN

Texas State Technical College
Internal Audit
Status of Fiscal Year 2019 Audit Schedule & Other Projects

| Description | Division/Campus | Status | Project No. | Report Date |
|---|-------------------------|-------------|-------------|---------------------------------|
| INTERNAL AUDITS | | | | |
| Facilities Development Project Compliance Audit | Facilities - West Texas | Complete | 19-006A | 11/28/18 |
| Facilities Development Project Compliance Audit | Facilities - Marshall | Complete | 19-007A | 11/28/18 |
| Google Drive Audit | OIT | Complete | 19-004A | 12/10/18 |
| TRS Contributions Audit | HR | Complete | 19-005A | 12/20/18 |
| Internal Penetration Test (North Texas) | OIT, North Texas Campus | Complete | 19-011A | 2/13/19 |
| Maxient Software | OIT, Student Discipline | Complete | 19-003A | 2/25/19 |
| Internal Penetration Test (Ft. Bend) | OIT, Ft. Bend Campus | Complete | 19-015A | 3/29/19 |
| Graduation Process Audit | Student Services | Complete | 19-008A | 4/9/19 |
| TAC §202 Compliance Audit | OIT | In Progress | 19-012A | 10/5/18, 1/11/19, 4/12/19 |
| Workplace Harassment Audit | HR | In Progress | | |
| Admissions Process Audit | Student Services | In Progress | | |
| Admissions IT Audit | Student Services/OIT | In Progress | | |
| Fixed Asset Control Follow-up Audit | Cross-Divisional | In Progress | | |
| C4EO Audit | C4EO | | | |
| Safety Follow-up Audit | Cross-Divisional | In Progress | | |
| Departmental Audit - Challenger Center | Harlingen | In Progress | | |
| Departmental Audit - Challenger Center | Waco | In Progress | | |
| TEC §51.9337 Contracting Audit | Purchasing | | | |

EXTERNAL AUDITS

| | | | | |
|--|--------------------------|--|--|---------|
| State Comptroller's Office: Desk Audit - Charge Card Program | Finance | Complete | | 8/27/18 |
| State Auditor's Office: A-133 Follow-up | Financial Aid - Marshall | Complete | | 2/28/19 |
| Single Audit for FY 2018: BKD | Accounting | Complete | | 2/12/19 |
| State Comptroller's Office: Post Payment Audit | Purchasing | Waiting on final report from Comptroller | | |
| TWC: Monitoring review of SDF Contract # 2418SDF002 | OSP/Harlingen | In Progress | | |
| TWC: Monitoring review of SDF Contract # 2418SDF003 | OSP/Harlingen | In Progress | | |

| Description | Division/Campus | Status | Project No. | Report Date |
|---|-----------------------------|----------|-------------|-------------|
| OTHER INTERNAL PROJECTS | | | | |
| Internal Ethics Line Report: An anonymous report indicated vending machines were charging more than the posted amount when a charge card was used. Results: We determined that when a card is used, a temporary transaction for \$1 more than the posted price is temporarily posted to the card holder's account, but the correct amount is charged when the customer's account is actually charged. Found the complaint to have no merit. | Business Services/Waco | Complete | 19-010P | 10/5/18 |
| Police Evidence Room Surprise Inspection | Police Department/Harlingen | Complete | 19-013A | 1/2/19 |
| Executive Management Request: Review contractual relationship with vendor associated with Helicopter Pilot Program, and any other potential exposure related to VA compliance. Results: Did not find any inappropriate training provided by the contractor. Identified several process improvements within accounting, tracking flight hours, and purchasing controls. | Instructional/Waco | Complete | 19-009I | 2/8/19 |
| SAO Ethics Line Report: An anonymous report indicated donations were being received and used by someone in the HVAC program that was not licensed to do so. Results: Allegation had no merit. HVAC programs receive small quantities of duct board. The product is not a restricted use item which requires special licensure. We did recommend that the donations be reported to the Foundation, though, as required by policy. | Instructional/Harlingen | Complete | 19-016I | 3/1/19 |
| Police Evidence Room Surprise Inspection | Police Department/Waco | Complete | 19-013A | 4/11/19 |

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 - North Texas (19-011A) | Security of information and assets could be improved by informing campus employees of the results of this project, and re-educating them on the risks we were able to exploit. | 2 people provided their credentials to the Portal, only 3 people reported our phishing to the Help Desk, and we were able to access areas that contained sensitive information without being detected. We also identified a wall jack with the cables exposed. | 1.1 All employees will be informed of the project results and reminded of their responsibilities to protect sensitive information and IT assets. Communication on the results and responsibilities will be delivered verbally (with discussion) at the scheduled Provost meeting for February and at each departmental meeting during February or March. Email communication on the results and responsibilities will also be sent in March to all employees as a follow up to the face to face meetings | Marcus Balch | 3/31/19 |
| | | | 1.2 IT has fixed the issue in Learning Resource Center room 118. A new wall plate has been installed to keep the cables in the wall. | Shelly Scherwitz/Adam Harvey | Immediately |



| Report Name & No. | Audit Finding | Summary of Finding Support | Management's CAP(s) | Resp. Sr Mgr | Expect. Complete Date |
|---|--|---|---|------------------------------|-----------------------|
| Audit of Maxient Application (19-003A) | While the majority of the minimally required TAC 202 controls are in place for the Maxient, we found 19 that still need attention. Those include deficiencies related to access and security. Since sensitive or important information is stored within the Maxient, we feel priority should first be given to access and security controls. | Identified excessive number of people with ADMIN access, no lockout setting after set # of login failures, no process for use of audit logs, no annual review of SOC2 report, and no annual risk assessment documentation. | 1.1 As noted in the report, a majority of the required controls have been implemented with the remaining controls being evaluated and addressed. For the controls not yet implemented, we are evaluating the associated risk to TSTC and associated applicability in our environment to prioritize implementation. IT Security along with TAC 202 compliance is a priority for TSTC to reasonably and effectively control risks. | Shelly Scherwitz/Adam Harvey | 7/31/19 |
| Internal Network Penetration Test - Ft. Bend (19-015A) | Security of information and assets could be improved by informing campus employees and the Office of Information Technology of the results of this project, and re-educating them on the risks we were able to exploit. | 3 people provided their credentials to the Portal, no one contacted the Help Desk to alert them of our phishing attempts, an IP address was printed on a publicly accessible printer which directed us to the security cameras, we were able to access the cameras, some network printers were open, and an open port was identified with access to the internal network. | 1.1 As expected, there were a few successful penetrations, while the majority of the attempts were thwarted. However, even one success can have disastrous consequences. I have received an out brief on the details of this exercise, and will use it as a learning experience for our employees, most of which are relatively new to TSTC. We have several opportunities to discuss these results, individually as well as in large and small group size. I will take advantage of these forums to discuss the mistakes individually with those who were "tricked" as well as the faculty and staff of the entire campus. | Randall Wooten | Immediately |

| Report Name & No. | Audit Finding | Summary of Finding Support | Management's CAP(s) | Resp. Sr. Mgr | Expect. Complete Date |
|-------------------|---------------|----------------------------|--|--------------------------------|-----------------------|
| | | | 1.2 Regarding the phone calls posing as helpdesk personnel, we do have Moodle training that was a requirement for employees to take for the academic year 2018/2019 titled "Information Security Awareness". There was a specific true/false question covering this very thing, and stated that "TSTC employees will never ask for your credentials over the phone or over email." TSTC / OIT will resend that required training back out to our users as a refresher. | Shelly Scherwitz/Brannon Suggs | Immediately |
| | | | 1.3 Cameras user account: vulnerability A TDX helpdesk ticket was created to resolve the camera user account issues. Reference: Ticket ID 8750411. It was marked as resolved Tue 3/19/19 8:14 AM. | Shelly Scherwitz/Brannon Suggs | Immediately |
| | | | 1.4 Printer user account vulnerability: A TDX helpdesk ticket was created to resolve these printer user account issues. Reference: Ticket ID 811618. | Shelly Scherwitz/Brannon Suggs | Immediately |
| | | | 1.5 Open Port - Ports have been disabled. | Shelly Scherwitz/Brannon Suggs | Immediately |

| Report Name & No. | Audit Finding | Summary of Finding Support | Management's CAP(s) | Resp. Sr Mgr | Expect. Complete Date |
|---|--|---|--|---|-----------------------|
| Graduation Process Audit (19-008A) | 1. Internal controls need to be improved to ensure certification requirements are always met, and well documented. | Signed certification of graduation document missing from 38 students, documentation of communications to students needs to be improved, and some graduates are not reported to the THECB. | 1.1 Management has implemented controls that include a centralized processing center to oversee the graduation process for all campuses. The standardization of these procedures should minimize any gaps in documentation standards. This new process will also ensure consistency in communication and information that is provided to respective graduates. 1.2 Management has implemented changes to the Graduation Policy removing the requirement to apply. This should minimize any issues with students not being reported to Texas Higher Education Coordinating Board. Centralization of certification and quality assurance checks should also minimize issues with reporting and reconciliation issues. | Christine Stuart-Carruthers/Paula Arredondo | 12/31/19 |
| | | | | Christine Stuart-Carruthers/Paula Arredondo | 8/31/19 |

| | |
|--|--|
| TAC 202 Compliance – Quarterly Update (19-012A) | No change in the number of implemented controls or controls pending review from the last quarter. In the 2nd quarter, management focused their attention on 8 outstanding PCI controls. Those controls are also pending Internal Audit review. |
|--|--|

| | |
|--|-------------------------------|
| Audit of Police Evidence Room – Waco Campus (19-013A) | No material exceptions noted. |
|--|-------------------------------|

| Report Name & No. | Audit Finding | Summary of Finding Support | Management's CAP(s) | Resp. Sr Mgr | Expect. Complete Date |
|--|---|----------------------------|---------------------|--------------|-----------------------|
| Single Audit - FY 2018 Financial Statements & Federal Compliance by BKD | FY 2018 Financial statement presented fairly in all material respects, no compliance issues identified with the review of Federal Financial Aid and Perkins funds, and no control deficiencies identified as they relate to financial reporting or the programs previously mentioned. | | | | |
| Federal Portion of the Statewide Audit Report for the Year Ended August 31, 2018 by State Auditor's Office | All corrective action plans were found to be fully implemented for deficiencies identified in 2014 . | | | | |

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

| Completion Summary | | | |
|---------------------------------|----------|---------|-------------------------------------|
| | 12/31/18 | 3/31/19 | Cleared from (Added to) Schedule |
| Audits from FY 2017 & Earlier | 3 | 3 | 0 |
| Audits from FY 2018 | 8 | 4 | 4 |
| Audits from 2019 | 2 | 7 | -5 |
| Total | 13 | 14 | -1 |
| Findings from FY 2017 & Earlier | 3 | 3 | 0 |
| Findings from FY 2018 | 8 | 4 | 4 |
| Findings Audits from 2019 | 2 | 7 | -5 |
| Total | 13 | 14 | -1 |
| CAPs from FY 2017 & Earlier | 3 | 3 | 0 |
| CAPS from FY 2018 | 12 | 6 | 6 |
| CAPS Audits from 2019 | 4 | 15 | -11 |
| Total | 19 | 24 | -5 |

Highlights:

| |
|---|
| Deficiencies in penetration tests (16-016A, 18-026A, and 18-046A) are projected to clear 8/23/19 once Active Directory is implemented. |
| Safety Audit (18-012A) has progressed with training, more standardization, survey, staff meetings, and hirings. |
| Inventory Issues noted in 17-013A are improving, with recent discussion on bar code scanner use and identifying fully depreciated, obsolete items still on the records. |
| TAC 202 & PCI controls are still progressing, with delays in noted improvement being due to Internal Audit still needing to test. |
| Deficiencies in penetration tests (18-011A & 18-015A) were corrected immediately, with verification pending by Internal Audit. |

| 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 |
|---|--|--|--|---|-----------------------------------|
| Internal Network Penetration Test (16-016A), Herrera | 1. We were able to find information on the internet that was useful to us in our social engineering attacks. As such, we were able to obtain both end-user credentials to systems containing protected data, and other information that could be used to get those credentials using relatively low-tech methods. We also noted instances in which physical security needs to be improved. Finally, we were able to inappropriately access student and employee data on servers using techniques available to more sophisticated hackers | We have reviewed the issues identified and agree that corrective actions are necessary. We formulated specific actions for each of the issues, and have already corrected some. All required actions will be completed no later than December 2016 since some actions will require assistance from personnel outside of OIT. | Substantially Complete: As of 7/7/17, 8 of 9 corrective action plans have been completed. The only item that is pending to be completed is CAP 2.1 relating to secured logons to lab computers. Dell One is currently being implemented. New anticipated date of completion is 5/31/19. No new updates as of 4/12/19. | Rick Collatos: The current Dell One Identity/AD project to address the findings for CAP 1.2 and CAP 2.1 in the previous audit findings will be a phased in approach for the Lab computers. The phased approach will begin June 2019 and complete August 23, 2019. | 5/31/2019 8/23/2019 |
| 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. | Partially Complete: During a follow-up in December 2018, we determined that the process of all stewards completing an annual inventory has significantly improved, as has the documentation of the disposed assets. The process for transferring assets from terminated/transferred stewards, and the process of updating asset records with the notes provided by stewards on their annual inventory sheets still need attention. On 4/8/19, met with leadership to discuss strategies to improve the process, to include using a bar code scanning system, and removing old, fully depreciated & obsolete items from the list | | 8/31/19 |

| Report Name & No., Resp. Sr Mgr | Internal Audit Finding | Management's CAP(s) | Internal Audit Comments on Status | Management Comments on Status | Expect. Complete Date |
|--|---|--|--|-------------------------------|-----------------------|
| TAC \$202 Compliance Audit (17-002A), Herrera | 1. Twenty-three of the 106 IT controls we tested have not yet been implemented. | As noted in the report, a majority of the required controls have been implemented with the remaining controls being evaluated and addressed. For the controls not yet implemented, we are evaluating the associated risk to TSTC and associated applicability in our environment to prioritize implementation. IT Security along with TAC 202 compliance is a priority for TSTC. | Ongoing: At 3/31/19, 99 controls were implemented, with 36 still requiring attention. 8 of those 36 controls are pending testing by Internal Audit. | | TBD |
| Application Process Investigation (18-0381), Herrera | 1. Summary: Admissions procedures need to be improved to ensure all applicants receive timely communication, and to ensure all internal and external reporting is accurate. | 1.1 The work performed by the Internal Audit Department further justifies our movement towards a centralized processing center where stricter internal controls and monitoring can take place. The recommendations for improvement are areas in which we are working to address. | Pending Review: At 4/12/19, Internal Audit is currently performing a full scope audit of the Admissions Process & Target X software. | | Pending Review |

| Report Name & No., Resp. Sr Mgr | Internal Audit Finding | Management's CAP(s) | Internal Audit Comments on Status | Management Comments on Status | Expect. Complete Date |
|--|---|---|--|-------------------------------|-----------------------|
| PCI Compliance Audit (18-009A), Herrera, Kilgore | 1. Numerous IT related controls and/or their control elements, as prescribed by PCI DSS, have not been implemented. As such, PCI DSS compliance is not being fully met. | 1.1 In an effort to ensure the protection of payment card data for students and employees, The Office of Information Technology has been working with Food Services to resolve a number of important control deficiencies during the audit and will continue to review and implement recommendations moving forward. As we anticipate that the review and implementation review of 100 controls across 6 objectives will take over a year, we will prioritize controls that have the largest impact on the protection of cardholder data. As part of this process, we will also implement the recommendation of an annual assessment of PCI-DSS controls to ensure ongoing adherence to PCI-DSS compliance changes. | Ongoing: As of 1/9/19, PCI controls were being mapped to TAC 202 controls so implementation efforts will be optimized. At 3/31/19, 8 controls were pending Internal Audit's review. | | 8/31/19 |

| | | | | | |
|--|--|--|----------------|---|-------------------------------------|
| Marshall: Internal Network Penetration Test (18-026A), Herrera, Kilgore | 1. Physical and logical security could be improved by informing campus employees of the results of this project, and re-educating them on the risks we were able to exploit. | 1.2 The Office of Information Technology is currently in the process of implementing a centralized computer management solution, Microsoft Active Directory, which will enable us to implement technical controls to enforce security on workstations. | Ongoing | Rick Collatos: The current Dell One Identity/AD project to address the findings for CAP 1.2 and CAP 2.1 in the previous audit findings will be a phased in approach for the Lab computers. The phased approach will begin June 2019 and complete August 23, 2019. | 12/31/2019, 8/23/2019 |
|--|--|--|----------------|---|-------------------------------------|

| Report Name & No., Resp. Sr Mgr | Internal Audit Finding | Management's CAP(s) | Internal Audit Comments on Status | Management Comments on Status | Expect. Complete Date |
|---|---|---|---|---|--------------------------------------|
| Safety & Security Audit (18-012A), Herrera | 1. Improvements should be made to standardize safety processes between campuses, and to better establish College expectations and accountability. | 1.1 We are currently reviewing all safety processes, and will be standardizing them throughout the State. Our efforts will, at a minimum, address all observations noted in the audit report and include follow-up of the individual safety issues notes at each campus as detailed in the supplemental report. The revised processes will include a designated safety officer performing frequent inspections, along with training individual departments. | Ongoing: As of 4/12/19 , safety and security training has taken place at each campus, a safety climate survey has been sent performed at each campus, a tracking schedule has been developed for outstanding issues, and a strategy for improving the overall safety process is well into the developmental phase. Furthermore, a dedicated safety employee has been hired in Waco, and a frequent meeting with safety personnel are being held to standardize process as appropriate. Internal Audit has participated in several meetings | | 8/31/19 |
| West Texas: Internal Network Penetration Test (18-046A), Herrera | 1. Security of information and assets could be improved by informing campus employees of the results of this project, and re-educating them on the risks we were able to exploit. | 1.2 The Office of Information Technology is currently in the process of implementing a centralized computer management solution, Microsoft Active Directory, which will enable us to implement technical controls to enforce security on workstations. We anticipate this project will be complete in the 2019 calendar year. | Ongoing | Rick Collatos: The current Dell One Identity/AD project to address the findings for CAP 1.2 and CAP 2.1 in the previous audit findings will be a phased in approach for the Lab computers. The phased approach will begin June 2019 and complete August 23, 2019. | 12/31/2019 , 8/23/2019 |
| Annual Compliance Audit of TEC §51.9337 (18-047A), Hockstra & Rushing | 2. We identified exceptions related to employee training on contracting procedures, conflict of interest procedures, the contract management handbook missing some current procedures, and some other documentation exceptions. | 2.1 Contract Management Training - Training for procurement staff and departments, as well as those with delegated authority to execute contracts will be conducted in November/December, following approval of statewide policy. | Partially Complete: Procurement staff were trained on 12/11/18 and 2/11/19. An email regarding the training via Moodle was sent to TSTC Designated Signatories on 4/11/19 instructing them to complete the training by 5/31/19. | | 12/31/2019 , 5/31/2019 |

| Report Name & No., Resp. Sr Mgr | Internal Audit Finding | Management's CAP(s) | Internal Audit Comments on Status | Management Comments on Status | Expect. Complete Date |
|--|---|---|--|-------------------------------|---|
| Audit of Google Drive (19-004A), Herrera | 1. While the majority of the minimally required TAC 202 controls are in place for the Google Drive, we found 12 that still need attention. Those include deficiencies related to access and security. Since sensitive or important information is stored within the Google Drive, we feel priority should first be given to access and security controls. | 1.1 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 to reasonably and effectively control risks. IT believes they can have these implemented by June 2019. | Ongoing | | 6/30/19 |
| Self-Audit of TRS Retirement Benefits Participation (19-005A), Hoekstra | 1. Processes related to employees electing ORP and processes related to TRS contributions for employees need improvement. | 1.1 A change will be made to implement a form to all New Hires and Re-Hires to complete with signatures of acknowledgement that signifies their ORP/TRS Eligibility and decision date. 1.2 When an employee is selected and approved to change positions from the COMP area of HR, they will be implementing procedures to notify an individual they have become eligible and will be followed up with a signed form from the employee of that acknowledgement. 1.3 A reconciliation will be performed at the end of each semester to ensure employees working 12 hours or less per week did not contribute to TRS. | Ongoing: At 4/12/19, the Compensation Department was still working on developing a form to document the ORP/TRS notification and employees election choice. IA will review again next quarter. Ongoing: At 4/12/19, the Compensation Department was still working on developing a form to document the ORP/TRS notification and employees election choice. IA will review again next quarter. | | 4/31/2019, 6/30/19 4/1/2019, 6/30/19 6/3/19 |

| 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 |
|--|---|---|--------------------------------------|----------------------------------|--------------------------|
| Internal Network Penetration Test - North Texas (19-011A), Herrera, Kilgore | 1. Security of information and assets could be improved by informing campus employees of the results of this project, and re-educating them on the risks we were able to exploit. | 1.1 All employees will be informed of the project results and reminded of their responsibilities to protect sensitive information and IT assets. Communication on the results and responsibilities will be delivered verbally (with discussion) at the scheduled Provost meeting for February and at each departmental meeting during February or March. Email communication on the results and responsibilities will also be sent in March to all employees as a follow up to the face to face meetings. | Pending Review | | 3/31/19 |
| | | 1.2 IT has fixed the issue in Learning Resource Center room 118. A new wall plate has been installed to keep the cables in the wall. | Pending Review | | Immediately |

| Report Name & No., Resp. Sr Mgr | Internal Audit Finding | Management's CAP(s) | Internal Audit Comments on Status | Management Comments on Status | Expect. Complete Date |
|---|---|--|-----------------------------------|-------------------------------|-----------------------|
| Audit of Maxient Application (19-003A), Herrera | 1. While the majority of the minimally required TAC 202 controls are in place for the Maxient, we found 19 that still need attention. Those include deficiencies related to access and security. Since sensitive or important information is stored within the Maxient, we feel priority should first be given to access and security controls. | 1.1 As noted in the report, a majority of the required controls have been implemented with the remaining controls being evaluated and addressed. For the controls not yet implemented, we are evaluating the associated risk to TSTC and the associated applicability in our environment to prioritize implementation. IT Security along with TAC 202 compliance is a priority for TSTC to reasonably and effectively control risks. | Ongoing | | 7/31/19 |

| | | | | | |
|--|--|---|----------------|--|-------------|
| Internal Network Penetration Test - Ft. Bend (19-015A), Herrera, Kilgore | 1. Security of information and assets could be improved by informing campus employees and the Office of Information Technology of the results of this project, and re-educating them on the risks we were able to exploit. | 1.1 As expected, there were a few successful penetrations, while the majority of the attempts were thwarted. However, even one success can have disastrous consequences. I have received an out brief on the details of this exercise, and will use it as a learning experience for our employees, most of which are relatively new to TSTC. We have several opportunities to discuss these results, individually as well as in large and small group size. I will take advantage of these forums to discuss the mistakes individually with those who were "tricked" as well as the faculty and staff of the entire campus. | Pending Review | | Immediately |
|--|--|---|----------------|--|-------------|

| Report Name & No., Resp. Sr Mgr | Internal Audit Finding | Management's CAP(s) | Internal Audit Comments on Status | Management Comments on Status | Expect. Complete Date |
|---------------------------------------|------------------------|--|--------------------------------------|----------------------------------|--------------------------|
| | | 1.2 Regarding the phone calls posing as helpdesk personnel, we do have Moodle training that was a requirement for employees to take for the academic year 2018/2019 titled "Information Security Awareness". There was a specific true/false question covering this very thing, and stated that "TSTC employees will never ask for your credentials over the phone or over email." TSTC / OIT will resend that required training back out to our users as a refresher. | Pending Review | | Immediately |
| | | 1.3 Cameras user account: vulnerability A TDX helpdesk ticket was created to resolve the camera user account issues. Reference: Ticket ID 8750411. It was marked as resolved Tue 3/19/19 8:14 AM. | Pending Review | | Immediately |
| | | 1.4 Printer user account vulnerability: A TDX helpdesk ticket was created to resolve these printer user account issues. Reference: Ticket ID 811618. | Pending Review | | Immediately |
| | | 1.5 Open Port - Ports have been disabled. | Pending Review | | Immediately |

| Report Name & No., Resp. Sr Mgr | Internal Audit Finding | Management's CAP(s) | Internal Audit Comments on Status | Management Comments on Status | Expect. Complete Date |
|--|--|--|--------------------------------------|----------------------------------|--------------------------|
| Graduation Process Audit (19-008A), Herrera | 1. Internal controls need to be improved to ensure certification requirements are always met, and well documented. | 1.1 Management has implemented controls that include a centralized processing center to oversee the graduation process for all campuses. The standardization of these procedures should minimize any gaps in documentation standards. This new process will also ensure consistency in communication and information that is provided to respective graduates. 1.2 Management has implemented changes to the Graduation Policy removing the requirement to apply. This should minimize any issues with students not being reported to Texas Higher Education Coordinating Board. Centralization of certification and quality assurance checks should also minimize issues with reporting and reconciliation issues. | Ongoing | | 12/31/19 |
| | | | Ongoing | | 8/31/19 |

| Report Name & No., Resp. Sr Mgr | Internal Audit Finding | Management's CAP(s) | Internal Audit Comments on Status | Management Comments on Status | Expect. Complete Date |
|--|---|--|-----------------------------------|-------------------------------|-----------------------|
| Helicopter Training Program Investigation (1-0091), 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. | Pending Review | | Immediately |

Internal Audit Department

Audit Report

Internal Network Penetration Test Audit (19-011A)
TEXAS STATE TECHNICAL COLLEGE
North Texas Campus

February 13, 2019

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 November 1, 2018 and December 1, 2018, we performed vulnerability scans and penetration testing of the College's internal network on the campus in North Texas.

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 North Texas 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) 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 so as to identify sensitive information or assets we could potentially pilfer. We attempted to gain access to privileged systems and information by scanning the network to identify control flaws, testing wireless access, and searching for available ports that we could plug in to. Finally, we accessed computers available to the public to determine whether we could gain access to sensitive information. Both manual and automated testing methods were used to detect and/or exploit vulnerabilities. Industry standards noted in the Scope & Methodology section of this report served as our basis.

We determined that employees are generally vigilant in protecting sensitive information during social engineering attempts, sensitive information was not exposed by them disposing of documents within recycle/trash bins or leaving documents in public view, and they use password protected screensavers on their machines when they are not at their desks. Some employees did report our phishing attempts, and the IT Help Desk has established protocols for notifying the campus of current attacks to minimize success. We verified that wireless access signals are generally confined to the campus with minimal room to restrict that access, guest networks are segregated from internal networks, and access to internal networks and systems are protected through secured logon protocols and encryption. We also found that access to networking closets were restricted by locks that required a key to open.

We did find opportunities for improvement. We were able to obtain user credentials through our phishing attempts, and identified improper handling of user password information indicating refresher training related these types of risks is warranted. And, we were able to access restricted areas after hours which allowed access to sensitive information.

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

Introduction

The Office of Information Technology (OIT) Division, overseen by the Vice Chancellor/Chief Student Services Officer, consists of 2 departments – the IT Support Operations Department with a staff of 45, the Department of Infrastructure Operations with a staff of 22. OIT assists the College with its operational needs by maintaining secure IT networks, providing end-user support and training, assisting with IT purchases, and maintaining critical databases and offering critical application support. We worked with the Enterprise Application Support Manager to create a realistic phishing email. OIT personnel were only notified when accounts were compromised or immediate remediation was required.

To ensure the integrity of the results, limited people were notified of our tests prior to us performing them. We notified the Provost on the North Texas campus of our project, but the specifics and timing of our tests were not disclosed. We attempted to make this test as realistic as possible to achieve reliable results.

In FY 2015, an external test was performed which simulated attacks from off-campus sites through the internet by a consultant. This test on-campus attacks by exploiting risks identified through first hand observations and research through resources available to anyone.

Objectives

The objectives of the internal network penetration test were to:

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

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

Scope & Methodology

The scope of the penetration test included the physical and logical securities of core network equipment, access network equipment, and servers located on the North Texas 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 were unwilling to disclose personal information and passwords, and OIT was responsive to when attacks were reported. Wired and wireless networks are segregated between privileged and guest accounts, with services generally 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 containing networking equipment were kept locked during and after business hours. There were not any network access ports in the building common areas, such as the student lounge, study area on second floor, or hallways.

Summary of Findings

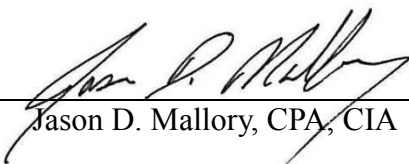
Security of information and assets could be improved by informing campus employees of the results of this project, and re-educating them on the risks we were able to exploit.

Opinion

Based on the audit work performed, IT assets and information are generally well protected on the North Texas campus. But, we identified some security issues that need to be improved. Those specific issues are included in a confidential supplemental report issued to the campus Provost and OIT.

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

February 13, 2019

Date

AUDIT FINDING DETAIL

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

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

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

Consequences: Failure to address the vulnerabilities exposes sensitive information to being lost and/or compromised.

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

Management Response:

Division: Office of Information Technology

Executive Management: Ricardo Herrera, VC/CSSO
Jeff Kilgore, VC/CAO

| Task | Brief Description | Responsible Individual | Completion Date |
|------|--|------------------------|-----------------|
| 1.1 | All employees will be informed of the project results and reminded of their responsibilities to protect sensitive information and IT assets. Communication on the results and responsibilities will be delivered verbally (with discussion) at the scheduled Provost meeting for February and at each departmental meeting during February or March. Email communication on the results and responsibilities will also be sent in March to all | Marcus Balch | March 31, 2019 |

| Task | Brief Description | Responsible Individual | Completion Date |
|------|--|------------------------|-----------------|
| | employees as a follow up to the face to face meetings. | | |
| 1.2 | IT has fixed the issue in Learning Resource Center room 118. A new wall plate has been installed to keep the cables in the wall. | Adam Harvey | Immediately |

Internal Audit Department

Audit Report

Audit of the Maxient Application (19-003A)
Of
TEXAS STATE TECHNICAL COLLEGE

February 25, 2019

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 Maxient Application (Maxient) as of July 31, 2018. The audit focused on application controls required in Texas Administrative Code 202 (TAC 202). Fifty one controls in 13 TAC domains were tested. We verified system access, periodical maintenance, training, audit logs, and baseline configurations. We also tested controls related to access, security awareness and training, audit and accountability safeguards, configuration management, and contingency planning. Finally, we tested media protection, risk assessment and purchasing processes, as well as system integrity.

The majority of the controls required by TAC 202 have been implemented. But, we identified 19 controls that still need to either be implemented or improved. We feel these issues warranted comment in this report to ensure future follow-up testing and correction. The following table summarizes the areas reviewed, and results:

| Control Family | Implemented | Implemented with Recommendations | Not Implemented | Required |
|--|-------------|----------------------------------|-----------------|----------|
| Access Controls | 4 | 0 | 4 | 8 |
| Awareness and Training Controls | 2 | 1 | 0 | 3 |
| Audit and Accountability Controls | 6 | 0 | 3 | 9 |
| Configuration Management Controls | 0 | 0 | 4 | 4 |
| Contingency Planning Controls | 1 | 0 | 4 | 5 |
| Identification and Authentication Controls | 4 | 1 | 0 | 5 |
| Maintenance Controls | 2 | 0 | 0 | 2 |
| Media Protection Controls | 2 | 0 | 0 | 2 |
| Personnel Security Controls | 1 | 0 | 3 | 4 |
| Risk Assessment Controls | 0 | 0 | 1 | 1 |
| System and Services | 2 | 0 | 0 | 2 |

| | | | | |
|---|-----------|----------|-----------|-----------|
| Acquisition Controls | | | | |
| System and Communications Protection Controls | 3 | 0 | 0 | 3 |
| System and Information Integrity Controls | 3 | 0 | 0 | 3 |
| Total | 30 | 2 | 19 | 51 |

Introduction

The College implemented Maxient, a cloud based application, in June 2015. Costs associated with the application include an initial setup fee of \$7,000 and an annual service fee of \$10,000 that renews automatically each year.

Maxient is used to report and track student conduct and behavioral incidents. Very sensitive information related to individual behavioral issues are stored within this database causing security of the data to be especially important. Currently, there are 39 users with access to Maxient, including members from the Behavioral Intervention Team (BIT), law enforcement officers, the Community Standards Liaison, as well as other instructional departments working directly with students. In addition, because user licensing is not restricted, the College can grant access to an unlimited number of users.

Maxient is a “Software as a Service” application, meaning the vendor hosts the application on their servers and is responsible for all maintenance. Those servers primarily reside on the East Coast. Users are able to access the application from any computer having internet connectivity, a current user ID and password.

The Maxient application contains 10 users with administrator access, however only 4 of these users are responsible for access and management of the application. The users consist of two Application Administrators within the Office of Information Technology, the Community Standards Liaison, and the Executive Director of Student Rights and Responsibilities which is overseen by the Support Center Director within the IT Support Operations Department (OIT).

Objectives

The objective of the audit was to ensure minimum application level controls, especially security related ones, are in place and working as intended for Maxient as required by TAC 202.

Scope & Methodology

The scope of our audit included all minimally required TAC 202 application controls as it relates to Maxient. The Texas Department of Information Resources (DIR) Security Controls Standards Catalog, NIST Special Publication 800-53A revision 4, and the DIR Texas Cloud Services Guide for State Agencies and Institutions of Higher Education formed the basis of our testing. To accomplish our objectives, we reviewed access, policies, system configurations, and other related information.

General Observations

Management thoroughly investigated and vetted various cloud based software programs for managing student behavior and records, with Maxient ultimately being chosen. Maxient includes detailed audit logs that are restricted to application administrators, and include sufficient information for action to be taken should an anomaly or issue surface. Security awareness training is provided to users, and role based security training is provided to application administrators. In addition, users can only access the application with the proper identification or authentication. Maxient is easily accessed by any of 3 web browsers; Chrome, Fire Fox, and Internet Explorer. The application has the ability to go back to reports generated to show time stamps of who generated and printed the report for detailed audit logs.

Summary of Finding

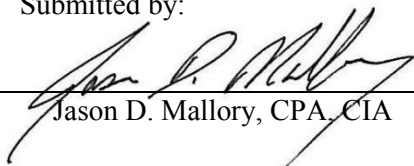
While the majority of the minimally required TAC 202 controls are in place for the Maxient, we found 19 that still need attention. Those include deficiencies related to access and security. Since sensitive or important information is stored within the Maxient, we feel priority should first be given to access and security controls.

Opinion

Based on the audit work performed, the majority of the required minimum information security controls have been implemented, but management needs to implement the remaining 19 controls, with priority first given to the ones related to access and security. The details of the controls and our results were provided to management in a separate document. They are not detailed in this report so as to limit risk associated with the deficiencies. The details are available upon request

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

February 25, 2019

Date

AUDIT FINDING DETAIL

Finding #1: While the majority of the minimally required TAC 202 controls are in place for the Maxient, we found 19 that still need attention. Those include deficiencies related to access and security. Since sensitive or important information is stored within the Maxient, we feel priority should first be given to access and security controls.

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

We determined that the majority of the information security controls were implemented; however, not all of the required controls were implemented by the required date. Controls in the following families were found to be either not implemented, or deficient:

| Control Family | Not Implemented |
|-----------------------------------|-----------------|
| Access Controls | 4 |
| Audit and Accountability Controls | 3 |
| Configuration Management Controls | 4 |
| Contingency Planning Controls | 4 |
| Personnel Security Controls | 3 |
| Risk Assessment Controls | 1 |
| Total | 19 |

Consequences: Being out of compliance with TAC 202 controls increases the likelihood of data leaks, data exfiltration, data deletion, account breaches, malware, and malicious insider attacks.

Possible Solution: We recommend the specific control deficiencies provided to management for the Maxient application be implemented.

Management Response:

Division: Office of Information Technology

Executive Management: Ricardo Herrera, Vice Chancellor & Chief Student Services Officer
Shelli Scherwitz, EVP/OIT

| Task | Brief Description | Responsible Individual | Completion Date |
|------|---|------------------------|-----------------|
| 1.1 | As noted in the report, a majority of the required controls have been implemented with the remaining controls being evaluated and addressed. For the controls not yet implemented, we are | Adam Harvey | July 31, 2019 |

| Task | Brief Description | Responsible Individual | Completion Date |
|------|--|------------------------|-----------------|
| | 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 to reasonably and effectively control risks. | | |

Internal Audit Department

Audit Report

Internal Network Penetration Test Audit (19-015A)
TEXAS STATE TECHNICAL COLLEGE
Fort Bend Campus

March 29, 2019

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 January 14, 2019 and February 28, 2019, we performed vulnerability scans and penetration testing of the College's internal network on the Fort Bend 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 Fort Bend 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) 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 available ports that we could plug in to. Finally, we accessed computers available to the public to determine whether we could gain access to sensitive information. Both manual and automated testing methods were used to detect and/or exploit vulnerabilities. Industry standards noted in the Scope & Methodology section of this report served as our basis.

We determined that employees are generally vigilant in protecting sensitive information during social engineering attempts, sensitive information was not exposed by them disposing of documents within recycle/trash bins or leaving documents in public view, and they use password protected screensavers on their machines when they are not at their desks. IT Help Desk has established protocols for notifying the campus of current attacks to minimize success. We verified that wireless access signals are confined to the campus with minimal room to restrict that access, guest networks are segregated from internal networks, and access to internal networks and systems are protected through secured logon protocols and encryption. We also determined that access to networking closets were restricted by locks that required a key and badge swipe combination in order to enter.

Nevertheless, we identified opportunities for improvement. We were able to obtain user credentials through our phishing and social engineering attempts, and identified different devices on the network devices that were using default passwords and no passwords at all. We were also able to access an open port, giving us the opportunity to perform scans on the internal network.

These opportunities for improvement can be addressed by reminding employees of their responsibilities to be vigilant for attempts to access sensitive information, and by establishing secure logon access to network devices accordingly. The College currently has policies which address both gaps we identified. A confidential supplemental report is available describing the specific vulnerabilities we identified.

Introduction

The Office of Information Technology (OIT) Division, overseen by the Vice Chancellor/Chief Student Services Officer, consists of 2 departments – the IT Support Operations Department with a staff of 45, the Department of Infrastructure Operations with a staff of 22. OIT assists the College with its operational needs by maintaining secure IT networks, providing end-user support and training, assisting with IT purchases, and maintaining critical databases and offering critical application support. We worked with the Enterprise Application Support Manager to create a realistic phishing email. OIT personnel were only notified when accounts were compromised or immediate remediation was required.

To ensure the integrity of the results, limited people were notified of our tests prior to us performing them. We notified the Provost on the Fort Bend campus of our project, but the specifics and timing of our tests were not disclosed. We attempted to make this test as realistic as possible to achieve reliable results.

In FY 2015, an external test was performed which simulated attacks from off-campus sites through the internet by a consultant. This test on-campus attacks by exploiting risks identified through first hand observations and research through resources available to anyone.

Objectives

The objectives of the internal network penetration test were to:

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

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

Scope & Methodology

The scope of the penetration test included the physical and logical securities of core network equipment, access network equipment, and servers located on the Fort Bend 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 were vigilant in protecting sensitive information, and access to it. Wired and wireless networks are segregated between privileged and guest accounts, with services generally 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 buildings. Access to closets containing networking equipment were kept locked during and after business hours. While away from their offices employees kept computers secured with password protected screen savers.

Summary of Findings

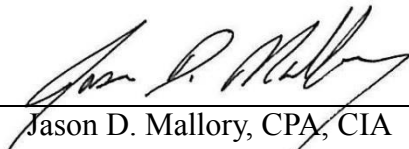
Security of information and assets could be improved by informing campus employees and the Office of Information Technology of the results of this project, and re-educating them on the risks we were able to exploit.

Opinion

Based on the audit work performed, IT assets and information are generally well protected on the Fort Bend campus, but we identified some security issues that need to be improved. Those specific issues are included in a confidential supplemental report issued to the campus Provost and OIT.

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

March 29, 2019

 Date

AUDIT FINDING DETAIL

Finding #1: Security of information and assets could be improved by informing campus employees and the Office of Information Technology of the results of this project, and re-educating them on the risks we were able to exploit.

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

While many controls are in place, we did identify areas that need to be improved. Specifically, employees need to be reminded of their responsibilities to protect information, some devices on the network need to be better protected through the use of strong passwords, and at least one open port needs to be disconnected from the internal network. The details of this finding are included in the Supplemental Audit Report rather than here so as to not create further risk. Please refer to that report for the support of this finding.

Consequences: Failure to address the vulnerabilities exposes student and employee sensitive information from being lost and or compromised.

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

Management Response: **Division:** Office of Information Technology

Executive Management: Ricardo Herrera, VC/CSSO
Jeff Kilgore, VC/CAO

Senior Management: Shelli Sherwitz, Sr. Director/ IT Support Operations
Randall Wooten, Provost/Fort Bend

| Task | Brief Description | Responsible Individual | Completion Date |
|------|---|------------------------|-----------------|
| 1.1 | In February 2019, the TSTC Audit Department perpetrated upon the Fort Bend County Campus, an internal Penetration Test to determine our susceptibility to compromise IT | Randall Wooten | Immediately |

| Task | Brief Description | Responsible Individual | Completion Date |
|------|---|------------------------|--------------------|
| | <p>and communication systems from outside sources. There was no prior warning or notification to anyone on the campus except myself. As expected, there were a few successful penetrations, while the majority of the attempts were thwarted. However, even one success can have disastrous consequences.</p> <p>I have received an out brief on the details of this exercise, and will use it as a learning experience for our employees, most of which are relatively new to TSTC. We have several opportunities to discuss these results, individually as well as in large and small group size. I will take advantage of these forums to discuss the mistakes individually with those who were “tricked” as well as the faculty and staff of the entire campus.</p> | | |
| 1.2 | Regarding the phone calls posing as helpdesk personnel, we do have Moodle training that was a requirement for employees to take for the academic year 2018/2019 titled "Information Security Awareness". There was a specific true/false question covering this very thing, and stated that "TSTC employees will never ask for your credentials over the phone or over email." TSTC / OIT will resend that required training back out to our users as a refresher. | Brannon Suggs | Immediately |
| 1.3 | <p>Cameras user account vulnerability</p> <p>A TDX helpdesk ticket was created to resolve the camera user account issues.</p> <p>Reference: Ticket ID 8750411</p> <p>It was marked as resolved Tue 3/19/19 8:14 AM</p> | Brannon Suggs | Resolved 3/19/2019 |
| 1.4 | <p>Printer user account vulnerability</p> <p>A TDX helpdesk ticket was created to resolve these printer user account issues.</p> <p>Reference: Ticket ID 8811618</p> | Brannon Suggs | Immediately |

| Task | Brief Description | Responsible Individual | Completion Date |
|------|--|------------------------|-----------------|
| | This ticket is still in progress, I will follow it to be sure it is completed | | |
| 1.5 | Summary: We are evaluating the open port availability, and have created a help desk ticket to address it. Reference: Ticket ID 8813238 | Brannon Suggs | Immediately |

Internal Audit Department

Audit Report

Graduation Process Audit (19-008A) **TEXAS STATE TECHNICAL COLLEGE**

April 9, 2019

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

Executive Summary

We completed an audit of the graduation process as of October 31, 2018. The primary purpose of this audit was to verify only qualified candidates who have satisfied all educational requirements were permitted to graduate. It was also intended to verify transactions and processes related to the graduation ceremony were reasonable and appropriate, and that diplomas and transcripts were released to only certified graduates who paid financial obligations and satisfied outstanding disciplinary issues.

To accomplish our objectives, we reviewed a sample of recent graduates from each campus from Fall 2017 through Summer 2018 to verify not only that their individual educational program requirements were met, but that internal controls were in place to ensure the requirements are met going forward. Our testing included grades, the process for identifying, reviewing, and certifying graduation candidates, system access, and communications related to graduating and the graduation ceremony. We also reviewed the accuracy of reporting to the Texas Higher Education Coordinating Board (THECB). SOS ES 4.17 Requirements for Graduation, SOS ES 4.25 Regulatory Reporting and Student Educational Services, and the Higher Education Coordinating Act of 1965 formed the basis of our compliance related testing.

We determined that the College maintains an accurate inventory of degree and certification programs, and has implemented controls to ensure educational requirements are being met by candidates prior to them being recognized as TSTC graduates. We were able to verify grades are recorded by the instructors of record. Generally, the Colleague EVAL tables critical to the graduation process accurately reflect the core educational program requirements as documented in the respective Course catalogs, and student records in Colleague are being updated to reflect graduate statuses. The THECB reporting is materially accurate and timely. Finally, students are afforded the opportunity to attend graduation ceremonies, with expenditures for those ceremonies being reasonable for the occasion.

But, we found controls and processes that need to be improved. Our testing identified the following:

- We found inconsistent documentation practices across campuses, and the need to better document graduation related communications with students.
- The 2017 & 2018 CBM009 reports for select campuses sent to the THECB did not reconcile to supporting information provided by the Registrar's Office.

Introduction

The Statewide Operating Standard (SOS) ES 4.17 Requirements for Graduation outlines the graduation requirements students must satisfy to be designated as graduates. To be certified as a graduate, a student must satisfactorily complete all required coursework, earn a "C" or better in all major-related courses, complete at least 25% of total required credit

hours at the College, and have a cumulative GPA of at least 2.0. Furthermore, all outstanding debts must be paid, and, if applicable, outstanding disciplinary issues resolved prior to diplomas and/or transcripts being released to graduates.

The Registrar's Office (Registrar) is responsible for verifying the requirements are met for each student prior to them being certified as a graduate. The Colleague EVAL report is the primary tool used in this certification. Currently, one employee is responsible for certifying all graduates. Other staff within the Registrar will assist as needed given the tight deadlines for certification. The Colleague EVAL report is the primary tool used in certifying graduates, along with various other documentation maintained in Colleague and the image system.

The College makes the graduation ceremony available to all qualified students, and makes every attempt to present actual diplomas to each graduate at that ceremony. In FY 2018, approximately \$100 thousand was expended on the ceremonies. The majority of those costs were related to venue rentals, and the purchases of diploma covers, diploma paper, printing services, and multi-media services. As expected, the amount of the costs attributed to each campus corresponded to the number of graduates, with the Harlingen and Waco campuses comprising the majority.

Graduate data is submitted annually to the THECB by the Business Analytics & Reporting Office, with assistance from the Registrar. Awards are a part of the College's appropriated funding formula, so inaccurate information could have a financial impact. The total number of degrees and certificates reported 2011 through 2018 follows:

Awards Conferred

| Fiscal Year | 2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011 |
|----------------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|
| Academic Year | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010 |
| Fort Bend | 132 | 87 | 13 | N/A | N/A | N/A | N/A | N/A |
| Harlingen | 1,148 | 1,195 | 1,146 | 1,197 | 966 | 825 | 807 | 693 |
| Marshall | 201 | 170 | 154 | 159 | 171 | 169 | 201 | 215 |
| North Texas | 85 | 64 | 28 | N/A | N/A | N/A | N/A | N/A |
| Waco | 1,393 | 1,417 | 1,259 | 1,235 | 1,147 | 1,219 | 1,266 | 1,098 |
| West Texas | 369 | 374 | 349 | 396 | 402 | 328 | 333 | 354 |
| Total | 3,328 | 3,307 | 2,949 | 2,987 | 2,686 | 2,541 | 2,607 | 2,360 |

Objectives

The primary purpose of this audit was to verify through substantive and control testing that graduates satisfy all educational requirements. We also verified diplomas and transcripts were released only to those graduates who paid all outstanding financial obligations, and resolved disciplinary matters. Secondary objectives included verifying students were afforded an opportunity to participate in memorable graduation ceremonies and those

related costs were reasonable. We also verified required reporting to the THECB is timely and accurate, and the graduation process as a whole is standardized across campuses.

Scope & Methodology

The scope of our audit included all degree and certificate candidates from the Fall 2017 through Summer 2018 semesters, and all transactions associated with certifying those students. To accomplish our objectives, we reviewed a sample of recent graduates from each campus to verify their individual educational program requirements were met. We also tested internal controls that ensure the integrity of the graduation results going forward. Grades, the process for identifying, reviewing and certifying candidates, system access, and related communications were all tested. We also reviewed the accuracy of reporting to the Texas Higher Education Coordinating Board (THECB). SOS ES 4.17 Requirements for Graduation, SOS ES 4.25 Regulatory Reporting and Student Educational Services, and the Higher Education Coordinating Act of 1965 formed the basis of our compliance related testing.

General Observations

One employee within the Registrar's Office is primarily responsible for certifying over a thousand awards each semester to almost as many students. Because the College has a goal of issuing diplomas to all graduates attending the graduation ceremony, there is considerable efforts on the parts of instructors to input final grades, and the Registrar to certify all students before the ceremony. There is typically less than a week from the end of the semester and the graduation ceremony. While the Registrar acknowledged that all students who are qualified to receive diplomas at the ceremony do not because of the number of graduates and limited time between the end of the semester and the ceremony, there is not a significant number. In fact, we observed a concerted effort to improve communication with those students who do not receive a diploma so that they understand the reason, and are not alarmed that they are not being recognized as graduates.

We noted an attitude of constant improvement among employees within the Registrar's Office, and the desire to perform the best work possible so that students and the College both succeed. Management was candid about processes that still needed to be improved. Single accreditation and the consolidation of processes have highlighted these needs, with efforts to improve being obvious.

As detailed in the Finding section of this report, we identified a need to continue improving internal controls. Many of the areas we identified were already receiving attention prior to this audit. An example of this related to rescinding the requirement that students *apply* for graduation before they are recognized as graduates. Beginning in Spring 2019, the policy was changed so that students would be credentialed by simply meeting the educational standards, regardless of whether they applied for graduation.

Summary of Finding

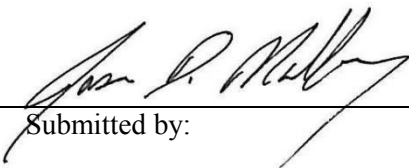
Internal controls need to be improved to ensure certification requirements are always met, and well documented.

Opinion

Based on the audit work performed, the College is only graduating students who have met educational requirements. We found a few instances of diplomas and/or transcripts being issued before all financial obligations were satisfied, but the total amount of the unpaid debts was less than \$3 thousand. Management addressed these issues and similar, less significant matters in a management letter. However, the effectiveness and efficiency of the graduation process would benefit from improving internal controls related to documenting certification and various communications to students.

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

Submitted by:


Submitted by:

April 9, 2019

AUDIT FINDING DETAIL

Finding #1: Internal controls need to be improved to ensure certification requirements are always met, and well documented.

Criterion: We selected a sample of 192 recent graduates statewide to verify they met all graduation standards, and were properly certified prior to being recognized as graduates and given diplomas. We performed a completeness test to ensure all qualified students were recognized as graduates. Students who graduated in the Fall 2017 through Summer 2018 semesters were in the scope of this audit. We also reviewed various graduation related communications to students to verify they were clear and well documented. Finally, we tested THECB graduate reporting for accuracy and timeliness.

We found the following deficiencies which led us to conclude controls need to be improved:

Documentation of graduate certification: The THECB requires a signed document be placed in each graduates permanent file. It documents the student met the graduation requirements, and those requirements were verified. Of the 192 we tested, 38 of these documents were missing from the students' files. There were other instances of the forms not being fully completed or containing inconsistent information.

General documentation standards: Throughout our testing, we identified gaps in documentation standards which prevented us from fully verifying various controls. The following observations were the most prevalent:

- The method of how/when the diploma was issued was inconsistently documented.
- Communications to students regarding graduating, the graduation ceremony, etc., were inconsistently documented.
- Letters rather than diplomas are occasionally handed to students at the graduation ceremony. Evidently there are various reasons for the letters. But because documentation is not maintained, we were unable to identify the number of people in recent ceremonies who have received these letters, and the reasons. Management indicated that the process has improved since Summer 2018.

THECB Reporting: We were unable to fully reconcile all students included on these reports to documentation generated by the College. The College has set forth a 2 week requirement to certify graduates. Because there are times students are certified beyond those 2 weeks, there are graduates that are subsequently never reported to the THECB as graduates. The lack of reporting could have an impact on appropriated funding.

Consequences: These observations increase the risk that errors are made.

Possible Solution: Enhance documentation standards and improve reporting processes to the THECB.

Management Response:

Division: Student Services

Executive Management: Rick Herrera

Senior Management: Dr. Christine Stuart-Carruthers

| Task | Brief Description | Responsible Individual | Completion Date |
|------|--|------------------------|-----------------|
| 1.1 | Management has implemented controls that include a centralized processing center to oversee the graduation process for all campuses. The standardization of these procedures should minimize any gaps in documentation standards. This new process will also ensure consistency in communication and information that is provided to respective graduates. | Registrar | December 2019 |
| 1.2 | Management has implemented changes to the Graduation Policy removing the requirement to apply. This should minimize any issues with students not being reported to Texas Higher Education Coordinating Board. Centralization of certification and quality assurance checks should also minimize issues with reporting and reconciliation issues. | Registrar | August 31, 2019 |

To: Shelli Scherwitz, Executive Vice President/OIT
 From: Jason D. Mallory, Audit Director
 Subject: TAC 202 Compliance – Quarterly Update
 Date: April 12, 2019

The purpose of this memo is to provide you the implementation statuses of IT controls required by TAC 202. The chart below provides a summary of the statuses, to include controls that your office has addressed, but my office has not yet had an opportunity to verify. It also shows the progress from the last quarter.

CURRENT RESULTS

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

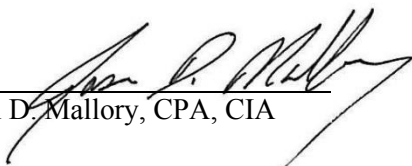
| | | | | | |
|--------------------------------------|------------|-------------|--------------|-------------|----------|
| Environmental Protection | | | | | |
| Planning | 1 | 0 | 2 | 3 | 0 |
| Program Management | 10 | 5 | 1 | 16 | 0 |
| Personnel Security | 2 | 4 | 2 | 8 | 2 |
| Risk Assessment | 2 | 1 | 1 | 4 | 0 |
| System and Services Acquisition | 3 | 1 | 3 | 7 | 0 |
| System and Communications Protection | 6 | 1 | 4 See note 1 | 11 | 0 |
| Security | 0 | 0 | 0 | 0 | 0 |
| System and Information Integrity | 2 | 1 | 3 | 6 | 0 |
| Transparency | 0 | 0 | 0 | 0 | 0 |
| Use Limitation | 0 | 0 | 0 | 0 | 0 |
| | | | | | |
| Total | 70 | 29 | 36 | 135 | 8 |
| | 52% | 21 % | 27% | 100% | |
| | | | | | |
| Previous Quarter Results | 70 | 29 | 36 | 135 | 8 |

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.

While no new TAC 202 controls are pending verification at this point, **8 new PCI controls were addressed this quarter, and are pending our review.** Progress is still being made in improving IT controls.

We appreciate your efforts, and encourage you to continue progressing with implementing the currently outstanding TAC 202 & PCI controls.

Submitted by:


 Jason D. Mallory, CPA, CIA

April 12, 2019

Date

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

Internal Audit Department

Audit Report

**Audit of Police Evidence Room (19-013A)
of
TEXAS STATE TECHNICAL COLLEGE
Waco Campus**

April 11, 2019

**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

On April 9, 2019, we performed a surprise inspection of the Police Department's evidence room (Room) on the Waco campus. Surprise inspections were requested by the Chiefs of Police as a way to verify all property is accounted for, and controls remain strong. The integrity of evidence is often crucial to the successful prosecution of crimes. And, because the Rooms contain illegal drugs and weapons confiscated during arrests, security is paramount.

The primary objectives of this audit were to ensure all evidence maintained in the Room in Waco was present and/or accounted for, and that access to the Room was restricted and monitored. We also verified that a process for destroying evidence has been implemented to ensure the Room does not become cluttered and disorganized over time. We accomplished these objectives by tracing samples, reviewing access and other detective controls, and observing the general organization and cleanliness of the Room and related documentation.

We were able to find all evidence we traced, and controls were adequate to ensure the contents are safeguarded from damage, loss, and theft. Additionally, the Room is well maintained, with sufficient evidence indicating property releases and destruction are being performed as appropriate.

Introduction

The Campus Police Department confiscates property during arrests and other incidences to hold as evidence in criminal proceedings. They also receive abandoned and lost property until the rightful owners can be located. All property is tagged with a case number and held in the evidence room.

The room contains illegal drugs (mostly marijuana), various weapons, to include guns and knives, and any other property that was confiscated or found. The room is restricted to only select police officers, with records maintained of all items that are stored in the room. Destruction or disposal of property tied to criminal cases occurs only after the respective district attorneys communicate a disposition of the case, and, for drugs and weapons, only after proper approval from the Court. All other property can be disposed after a specified timeframe. The police department disposes and/or destroys items from the evidence room 1-2 times a year, with the most recent disposal occurring in June 2018.

Objectives

The primary objectives of this audit were to ensure all evidence maintained in the Room was present and/or accounted for, and that access was restricted and monitored.

Scope & Methodology

The scope of our audit included all items stored in the Room as of April 9, 2019. To accomplish our objectives we traced samples of evidence noted in records to the actual items and vice versa, observed access and other safeguarding controls, and noted the general organization and cleanliness of each Room.

General Observations

Well-designed controls have been put in place over Police evidence to ensure its integrity and security. The Police are diligent in their efforts to limit access to the evidence and treat it as highly sensitive. Limited access, entry logs, sealed evidence bags, and card reader/picture notification for anyone entering the Room are the key controls. The Room is very organized.

Summary of Findings

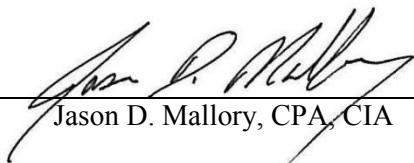
No material exceptions were identified.

Opinion

Based on the audit work performed, all Police evidence was present and/or accounted for, with access restricted and monitored.

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

Submitted by:


 Jason D. Mallory, CPA, CIA

April 11, 2019

Date

Independent Auditor's Report

The Board of Regents
Texas State Technical College
Waco, Texas

Report on the Financial Statements

We have audited the accompanying financial statements of Texas State Technical College (TSTC/College) as of and for the year ended August 31, 2018, and the related notes to the financial statements, which collectively comprise TSTC's basic financial statements listed in the table of contents.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on these financial statements based on our audit. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Governmental Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of TSTC as of August 31, 2018, and the changes in its financial position and its cash flows for the year then ended in accordance with accounting principles generally accepted in the United States of America.

Emphasis of Matter

As discussed in Note 12 to the financial statements, in 2018 TSTC adopted GASB No. 75, *Accounting and Financial Reporting for Postemployment Benefits Other Than Pensions*, and corrected the prior year capital assets balance. Our opinion is not modified with respect to this matter.

Other Matters

Required Supplementary Information

Accounting principles generally accepted in the United States of America require that pension and other postemployment information listed in the table of contents be presented to supplement the basic financial statements. Such information, although not part of the basic financial statements, is required by the Governmental Accounting Standards Board, who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic or historical context. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic financial statements and other knowledge we obtained during our audit of the basic financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Management has omitted the management's discussion and analysis information that accounting principles generally accepted in the United States of America require to be presented to supplement the basic financial statements. Such missing information, although not a part of the basic financial statements, is required by the Governmental Accounting Standards Board who considers it to be an essential part of the financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. Our opinion on the basic financial statement is not affected by the missing information.

Supplementary Information

Our audit was conducted for the purpose of forming an opinion on the financial statements that collectively comprise TSTC's basic financial statements. The accompanying supplementary information including the comparative statements of net position (August 31, 2018), the comparative statements of revenues, expenses and changes in net position (year ended August 31, 2018), matrix of operating expenses, changes in bonded indebtedness, state grant pass-through from state agencies and the schedule of expenditures of federal awards, as listed in the table of contents, are presented for purposes of additional analysis, and are not a required part of the basic financial statements. Such information is the responsibility of management and was derived from, and relates directly to, the underlying accounting

records used to prepare the basic financial statements. The supplementary information has been subjected to auditing procedures applied in the audit of the basic financial statements and certain additional procedures, including comparing and reconciling such information directly to the underlying accounting and other records used to prepare the basic financial statements or to the basic financial statements themselves, and other additional procedures in accordance with auditing standards generally accepted in the United States of America. In our opinion, the information is fairly stated in all material respects in relation to the basic financial statements as a whole.

Other Information

The comparative statements of net position and comparative statements of revenues, expenses and changes in net position as of and for the years ended August 31, 2017 and 2016, have not been subjected to auditing procedures applied in the audit of the basic financial statements and, accordingly, we express no opinion or other form of assurance on them.

Other Reporting Required by *Government Auditing Standards*

In accordance with *Government Auditing Standards*, we have also issued our report dated February 12, 2019, on our consideration of TSTC's internal control over financial reporting and on our tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements and other matters. The purpose of that report is solely to describe the scope of our testing of internal control over financial reporting and compliance and the results of that testing, and not to provide an opinion on the internal control over financial reporting or on compliance. That report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering TSTC's internal control over financial reporting and compliance.

BKD, LLP

San Antonio, Texas
February 12, 2019

**Report on Internal Control over Financial Reporting and on Compliance and
Other Matters Based on an Audit of Financial Statements Performed
in Accordance with *Government Auditing Standards***

Independent Auditor's Report

The Board of Regents
Texas State Technical College
Waco, Texas

We have audited, in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, the financial statements of Texas State Technical College (TSTC/College), which comprise the statement of net position as of August 31, 2018, and the related statements of revenues, expenses and changes in net position, and cash flows for the year then ended, and the related notes to the financial statements, and have issued our report thereon dated February 12, 2019, which contained an emphasis of matter paragraph for a change in accounting principle and a “Other Matter” paragraph regarding omission of required supplementary information.

Internal Control over Financial Reporting

In planning and performing our audit of the financial statements, we considered TSTC's internal control to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of TSTC's internal control. Accordingly, we do not express an opinion on the effectiveness of TSTC's internal control.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the College's financial statements will not be prevented, or detected and corrected. A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses or significant deficiencies. However, material weaknesses may exist that have not been identified.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether TSTC's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the College's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the College's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

BKD, LLP

San Antonio, Texas
February 12, 2019

Report on Compliance for Each Major Federal Program and Report on Internal Control over Compliance

Independent Auditor's Report

The Board of Regents
Texas State Technical College
Waco, Texas

Report on Compliance for Each Major Federal Program

We have audited Texas State Technical College's (TSTC/College) compliance with the types of compliance requirements described in the *OMB Compliance Supplement* that could have a direct and material effect on each of TSTC's major federal programs for the year ended August 31, 2018. TSTC's major federal programs are identified in the summary of auditor's results section of the accompanying schedule of findings and questioned costs.

Management's Responsibility

Management is responsible for compliance with federal statutes, regulations, contracts and the terms and conditions of its federal awards applicable to its federal programs.

Auditor's Responsibility

Our responsibility is to express an opinion on compliance for each of TSTC's major federal programs based on our audit of the types of compliance requirements referred to above. We conducted our audit of compliance in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and the audit requirements of Title 2 U.S. *Code of Federal Regulations* Part 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (Uniform Guidance). The College was not required by Uniform Guidance to have an audit, but requested an audit of major federal programs (as defined by Uniform Guidance) based on the compliance requirements in the *OMB Compliance Supplement*. Those standards and the Uniform Guidance require that we plan and perform the audit to obtain reasonable assurance about whether noncompliance with the types of compliance requirements referred to above that could have a direct and material effect on a major federal program occurred. An audit includes examining, on a test basis, evidence about TSTC's compliance with those requirements and performing such other procedures as we considered necessary in the circumstances.

We believe that our audit provides a reasonable basis for our opinion on compliance for each major federal program. However, our audit does not provide a legal determination of TSTC's compliance.

Opinion on Each Major Federal Program

In our opinion, TSTC complied, in all material respects, with the types of compliance requirements referred to above that could have a direct and material effect on each of its major federal programs for the year ended August 31, 2018.

Report on Internal Control over Compliance

Management of TSTC is responsible for establishing and maintaining effective internal control over compliance with the types of compliance requirements referred to above. In planning and performing our audit of compliance, we considered TSTC's internal control over compliance with the types of requirements that could have a direct and material effect on each major federal program to determine the auditing procedures that are appropriate in the circumstances for the purpose of expressing an opinion on compliance for each major federal program and to test and report on internal control over compliance in accordance with the Uniform Guidance, but not for the purpose of expressing an opinion on the effectiveness of internal control over compliance. Accordingly, we do not express an opinion on the effectiveness of TSTC's internal control over compliance.

A deficiency in internal control over compliance exists when the design or operation of a control over compliance does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, noncompliance with a type of compliance requirement of a federal program on a timely basis. *A material weakness in internal control over compliance* is a deficiency, or a combination of deficiencies, in internal control over compliance, such that there is a reasonable possibility that material noncompliance with a type of compliance requirement of a federal program will not be prevented, or detected and corrected, on a timely basis. *A significant deficiency in internal control over compliance* is a deficiency, or a combination of deficiencies, in internal control over compliance with a type of compliance requirement of a federal program that is less severe than a material weakness in internal control over compliance, yet important enough to merit attention by those charged with governance.

Our consideration of internal control over compliance was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over compliance that might be material weaknesses or significant deficiencies. We did not identify any deficiencies in internal control over compliance that we consider to be material weaknesses or significant deficiencies. However, material weaknesses may exist that have not been identified.

The purpose of this report on internal control over compliance is solely to describe the scope of our testing of internal control over compliance and the results of that testing based on the requirements of the Uniform Guidance. Accordingly, this report is not suitable for any other purpose.

BKD, LLP

San Antonio, Texas
February 12, 2019

Texas State Technical College
A Component Unit of the State of Texas
Schedule of Findings and Questioned Costs
Year Ended August 31, 2018

Summary of Auditor's Results

Financial Statements

1. The type of report the auditor issued on whether the financial statements audited were prepared in accordance with accounting principles generally accepted in the United States of America (GAAP) was:
☒ Unmodified ☐ Qualified ☐ Adverse ☐ Disclaimer

2. The independent auditor's report on internal control over financial reporting disclosed:
Significant deficiency(ies)? ☐ Yes ☒ None reported
Material weakness(es)? ☐ Yes ☒ No

3. Noncompliance considered material to the financial statements was disclosed by the audit? ☐ Yes ☒ No

Federal Awards

4. The independent auditor's report on internal control over compliance for major federal awards programs disclosed:
Significant deficiency(ies)? ☐ Yes ☒ None reported
Material weakness(es)? ☐ Yes ☒ No

5. The opinion expressed in the independent auditor's report on compliance with requirements that could have a direct and material effect on major federal awards was:
☒ Unmodified ☐ Qualified ☐ Adverse ☐ Disclaimer

Texas State Technical College
A Component Unit of the State of Texas
Schedule of Findings and Questioned Costs (Continued)
Year Ended August 31, 2018

6. The audit disclosed findings: ☐ Yes ☒ No

7. TSTC's major programs were:

| Cluster/Program | CFDA Number |
|---|-------------|
| Student Financial Assistance Cluster | |
| Federal Supplemental Educational Opportunity Grants | 84.007 |
| Federal Work-Study Program | 84.033 |
| Federal Pell Grant Program | 84.063 |
| Federal Direct Student Loans | 84.268 |
| Career and Technical Education – Basic Grants to States | 84.048 |

8. The threshold used to distinguish between Type A and Type B programs was \$1,769,411.

9. TSTC qualified as a low-risk auditee? ☐ Yes ☒ No

Texas State Technical College
A Component Unit of the State of Texas
Schedule of Findings and Questioned Costs (Continued)
Year Ended August 31, 2018

Findings Required to be Reported by *Government Auditing Standards*

| Reference Number | Finding |
|----------------------------|---------|
| No matters are reportable. | |

Findings Required to be Reported by the Uniform Guidance

| Reference Number | Finding |
|----------------------------|---------|
| No matters are reportable. | |

| |
|--|
| Texas State Technical College – Marshall |
|--|

Reference No. 2014-122

Eligibility**Student Financial Assistance Cluster**

Award year – July 1, 2013 to June 30, 2014

Award numbers – CFDA 84.007, Federal Supplemental Educational Opportunity Grants, P007A138753; CFDA 84.033, Federal Work-Study Program, P033A138753; CFDA 84.063, Federal Pell Grant Program, P063P135503; and CFDA 84.268, Federal Direct Student Loans, P268K135503

Type of finding – Significant Deficiency and Non-Compliance

Cost of Attendance

The determination of the federal student financial assistance award amount is based on financial need. Financial need is defined as a student's cost of attendance (COA) minus the expected family contribution (EFC) (Title 20, United States Code, Chapter 28, Subchapter IV, Section 1087kk). The phrase "cost of attendance" refers to the "tuition and fees normally assessed for a student carrying the same academic workload as determined by the institution, and including costs for rental or purchase of any equipment, materials, or supplies required of all students in the same course of study." An institution may also include an allowance for books, supplies, transportation, miscellaneous personal expenses, and room and board (Title 20, United States Code, Chapter 28, Subchapter IV, Section 1087ll).

| | |
|------------------------------|-------------|
| Initial Year Written: | 2014 |
| Status: | Implemented |
| U.S. Department of Education | |

For Title IV programs, the EFC is the amount a student and his or her family are expected to pay for educational expenses and is computed by the federal central processor and included on the student's Institutional Student Information Record (ISIR) provided to the institution. Awards must be coordinated among the various programs and with other federal and non-federal assistance to ensure that total assistance is not awarded in excess of the student's financial need (Title 34, Code of Federal Regulations (CFR), Sections 668.2 and 673.5).

For students with less-than-half-time enrollment, COA includes tuition and fees and an allowance for only books, supplies, and transportation; dependent care expenses; and room and board costs, except that a student may receive an allowance for such costs for not more than three semesters, or the equivalent, of which not more than two semesters or the equivalent may be consecutive (Higher Education Act of 1965 (HEA), Section 472(4)).

Texas State Technical College – Marshall (College) initially calculates student COA budgets based on full-time enrollment. After the census date each semester, the College identifies students with less-than-full-time enrollment and runs a process within its financial aid system, Colleague, to adjust those students' COA budgets. That process requires the College to manually enter specific award codes to adjust students' COA based on their enrollment.

For 5 (8 percent) of 60 students tested, the College did not correctly or consistently calculate COA. The five students were enrolled less than full-time, and the College did not adjust their COA after the census date based on their actual enrollment. That occurred because the College did not enter the correct award codes for those students, and Colleague did not identify that the COA needed to be adjusted. That resulted in overawards for 2 of those students totaling \$2,399 in Federal Direct Student Loans. After auditors brought those overawards to the University's attention, it corrected the overawards and returned the funds; therefore, there were no questioned costs.

Additionally, the College's COA budgets are not consistent with federal requirements. The College's COA budgets include a personal expense component for all students. However, the personal expense component is not allowable for students who are enrolled less than half-time. Two (3 percent) of 60 students tested were enrolled less than half-time, but the College assigned them a personal expense COA component that they were not eligible. That occurred because the College was not aware that less-than-half-time students were not eligible for a personal expense component. Although those two students were not overawarded student financial assistance, including COA components for which students are not eligible increases the risk that students could be overawarded student financial assistance.

Corrective Action:

Corrective action was taken.

Texas State Technical College
Internal Audit
Attestation Disclosures

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

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

