THE UNIVERSITY OF TEXAS-PAN AMERICAN
OFFICE OF AUDITS & CONSULTING SERVICES

Department of Criminal Justice

Report No. 15-13

OFFICE OF INTERNAL AUDITS

THE UNIVERSITY OF TEXAS - PAN AMERICAN

1201 West University Drive • Edinburg, Texas 78539-2999 • Office (956) 665-2110

July 31, 2015

Dr. Havidán Rodríguez, Interim President
The University of Texas-Pan American
1201 W. University Drive
Edinburg, TX 78539

Dear Dr. Rodríguez,

As part of our fiscal year 2015 Audit Plan, we completed a change in management audit of the Department of Criminal Justice. The objective of the audit was to evaluate the adequacy and effectiveness of the department's system of internal controls with an emphasis on financial and administrative controls. Our scope encompassed activity from September 1, 2013 through August 31, 2014.

Based on the work performed, we concluded that the department had a moderate system of financial and administrative controls. We identified areas where improvements could be made to internal controls. The detailed report is attached for your review.

We appreciate the courtesy and cooperation received from management and staff during our audit.

Sincerely,

Eloy R. Alaniz, Jr., CPA, CIA, CISA
Executive Director of Audits & Consulting Services

Table of Contents

EXECUTIVE SUMMARY _____ *1*

BACKGROUND _____ *2*

AUDIT OBJECTIVE _____ *2*

AUDIT SCOPE AND METHODOLOGY _____ *2*

AUDIT RESULTS _____ *3*

CONCLUSION _____ *7*

The University of Texas - Pan American
Department of Criminal Justice
Change in Management Audit

EXECUTIVE SUMMARY

The Department of Criminal Justice (department) provides a comprehensive education focused on crime and its control utilizing social science and interdisciplinary approaches. It prepares the student in the knowledge, skills and critical thinking needed to enter such careers as law enforcement, probation, parole, institutional corrections, youth services and police management at all levels of government. The interim chair assumed responsibility for the department on September 1, 2014.

As required by The University of Texas System's (System) *1996 Action Plan to Enhance Internal Controls,* a change in management audit is performed when a department undergoes a change in management or a significant change in reporting lines. The objective of the audit was to evaluate the adequacy and effectiveness of the department's system of internal controls with an emphasis on financial and administrative controls. The specific internal control areas we focused on included the control conscious environment, approval and authorization, segregation of duties, safeguarding of assets, monitoring and information technology.

Our scope encompassed activity from September 1, 2013 through August 31, 2014. The audit was conducted in accordance with guidelines set forth in The University of Texas System's Policy 129 and the *Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing.*

Overall, the department established a moderate system of financial and administrative internal controls. During the course of the audit we observed the following:

- A departmental policy and procedures manual was not developed;
- The department did not have a risk assessment;
- Not all required employee trainings and nepotism certifications were completed;
- Employee vacation and sick leave documentation was not maintained;
- Project account reconciliations were not signed off by the project manager to indicate that they were reviewed.
- Lack of monitoring for personally owned laptops and unencrypted portable storage devices;
- The department used an unencrypted portable storage device. No sensitive or confidential information was found on the tested device.

Beginning on September 1, 2015, The University of Texas at Brownsville and The University of Texas – Pan American will consolidate to create The University of Texas Rio Grande Valley (UTRGV). The Office of Internal Audits will follow-up with the UTRGV responsible party for this area to ensure that the issues identified in this audit are addressed and mitigated.

BACKGROUND

The Department of Criminal Justice offers a Bachelor's and Master's degree that probe into a proper understanding of crime and the criminal justice enterprise created to control it. This field of study not only examines crime and criminal justice issues, but also their social, ideological, and cultural foundations, and procedures toward initiating changes to reduce crime and modify criminal justice institutions toward the development of a good society for all. The department's mission is to impart knowledge and promote critical thinking about the crime problem, and its control through criminal justice institutions and public cooperation. The department works towards helping students develop the knowledge and analytical abilities to become agents of change.

The interim chair assumed responsibility for the department on September 1, 2014 (FY15). A summary of the department's project account's FY 2014 financial activity is summarized below.

Project Account	Budget	Encumbrances	Actual	Funds Available
140CJUS00	$1,216,031	$302	$1,215,297	$432
21CJUS000	$174	$0	$0	$174
24CJUS000	$4,509	$100	$3,916	$493
45CJUS000	$221	$0	$215	$6
Totals	**$1,220,935**	**$402**	**$1,219,428**	**$1,105**

AUDIT OBJECTIVE

The objective of the audit was to evaluate the adequacy and effectiveness of the department's system of internal controls with an emphasis on financial and administrative controls.

AUDIT SCOPE & METHODOLOGY

We evaluated the department's internal controls related to a control conscious environment, approval and authorization, segregation of duties, safeguarding of assets, as well as monitoring and information technology. Our scope included activity from fiscal year 2014 (September 1, 2013 through August 31, 2014). To accomplish the audit objective, we performed the following procedures:

- Interviewed the interim chair and discussed an internal control questionnaire to obtain an understanding of the department's operations and related internal controls.
- Interviewed employees for additional input on internal controls.
- Determined whether a control conscious environment was established, whether goals and objectives had been developed, and whether a risk assessment and implementation plan had been developed.
- Determined whether account reconciliations had been performed and approved on a timely basis and whether segregation of duties existed.

- Examined operating and financial information for reliability.
- Tested a sample of expenditures and examined supporting documentation for proper approval and authorization.
- Reviewed employee leave and tested timecards for proper approval and authorization.
- Performed property inventory testing for the existence of selected assets, and determined whether selected assets were properly recorded on the University's asset management system.
- Reviewed information security controls for portable drives.
- Verified compliance with the University's policies and procedures.

The audit was conducted in accordance with guidelines set forth in The University of Texas System's Policy UTS 129 – Internal Audit Activities and the *Institute of Internal Auditor's' International Standards for the Professional Practice of Internal Auditing.*

AUDIT RESULTS

Control Conscious Environment

A control conscious environment encompasses technical competence and ethical commitment, and is necessary for the establishment of effective internal controls. To establish an adequate control conscious environment, a department should have goals and objectives, a mission statement, a risk assessment and implementation plan, and a policies and procedures manual. These items should be reviewed regularly and updated as needed. Additionally, adequate training should be provided, performance evaluations should be conducted regularly, and any conflicts of interest should be identified and addressed.

The department had developed a mission statement, goals and objectives.

We tested 16 employees for completion of annual trainings and nepotism certification. Additionally, we tested one (1) employee to determine whether an annual performance evaluation had been performed. The results of our tests are as follows:

- 1 out of 16 (6%) employees did not complete their sexual harassment training
- 2 out of 16 (13%) employees did not complete their annual standards of conduct training
- 3 out of 16 (19%) employees did not complete their information security training
- 7 out of 16 (44%) employees did not complete a nepotism certification
- 1 out of 1 (100%) employees completed their annual performance evaluation (SEPAP)

Additionally, we noted that the department had not developed a policy and procedures manual and had also not conducted a risk assessment. A risk assessment was developed during the audit.

Based on testing, we found that the department established a moderate control conscious environment.

Approval & Authorization

Adequately established approval and authorization controls help to ensure that expenditures are allowable and appropriate. During the audit period, the former department chair was account manager for four (4) project accounts, with the administrative assistant listed as the project reviewer.

We reviewed operating, travel, and payroll expenditures to test for compliance with University procedures. We tested a sample of expenditures in each category and examined supporting documentation for proper approval, accuracy, and whether the expenditures were reasonable. The department did not utilize a procurement card during FY 2014.

Operating and Travel Expenditures

We judgmentally selected a sample of 20 operating and 10 travel transactions representing 49% and 47% of the total dollar value of the population, respectively. We found that expenditures were properly approved, appropriate, and supported with adequate documentation. No exceptions were noted.

Payroll and Employee Leave

We judgmentally selected five (5) employees to test for payroll accuracy. We verified that the employees' compensation agreed with their memoranda of employment. We determined that the payroll for employees tested was accurate.

We also evaluated the process for leave taken by employees, reconciliations of leave reports to the official University timecard, and ensured that timecards were properly approved. The department initially relied on e-mail notifications to document employee leave. Subsequently, the department implemented the use of the *Leave Approval Request* form. We tested one (1) employees' vacation and sick leave for the months of November and December 2013. Based on our employee leave test, we determined that all employee timecards were approved by their supervisor. However, the department was unable to provide any support documentation related to the employee sick and vacation leave.

Based on testing, we concluded that the department's internal controls over payroll and employee leave were moderate.

Safeguarding of Assets

Tangible assets, vital documents, critical systems, and confidential information must be safeguarded against unauthorized acquisition, use, or disposal. We performed property inventory testing to determine the existence of assets and whether assets were properly recorded on the Oracle Fixed Assets system.

We selected a sample of 10 assets with a historical cost greater than $1,100 to test for existence. We were able to locate all of the assets selected for testing. Additionally, we selected three (3) assets in the department to verify inclusion of the assets in the assets management system. We were able to trace all three (3) assets back to the inventory records. Additionally, we determined that the department did not handle university funds during FY 2014.

Based on testing, we determined that the department established adequate safeguarding of fixed asset controls.

Segregation of Duties

Adequate segregation of duties should be maintained between the people who authorize transactions, record transactions, and have custody of assets. We reviewed areas such as purchases, timecards, and statement of account reconciliations to evaluate segregation of duties.

The former department chair had signature/approval authority over the department's accounts, including account reconciliations, purchases, and timecards. Project accounts were set up with separate individuals listed as the project manager, project reviewer, and alternate approver. The department's administrative assistant was responsible for preparing account reconciliations, while the former chair was responsible for reviewing and approving the reconciliations. The department did not handle cash during FY 2014.

We found that adequate controls over segregation of duties for the areas evaluated were in place.

Monitoring

In accordance to Handbook of Operating Procedure Section 8.6.4: *Fiscal Accountability Policy*, project managers are responsible for providing assurance as to the accuracy of their accounts by certifying that the account has been reconciled for the fiscal year and that all reconciling items have been satisfactorily resolved. Without adequate monitoring of project account reconciliations, items that require attention may go unnoticed.

We reviewed two (2) months of account reconciliations. We determined that the tested account reconciliations were properly completed; however, we noticed that the former chair did not sign off on the completed reconciliations to indicate that they were reviewed. We were informed that

the former chair inquired about the account balances but did not perform a formal review of the account reconciliations.

We concluded that the department had moderate controls over account reconciliations.

Monitoring of personal electronic equipment (e.g. laptops, tablets, portable storage devices, etc.) should be conducted to ensure that proper safeguards are in place to prevent loss of mission critical data. All University laptops, including personally owned computers used for University business must be encrypted. Employees are responsible for contacting the Office of Privacy and Security about their use of personally owned laptops to conduct University business. They must encrypt their laptops or request assistance from the University Help Desk.

We inquired as to whether the department maintains information on employees that use personal laptops and unencrypted portable storage devices to conduct University business. We found that the department did not have a procedure in place for monitoring such equipment.

We concluded that the department had inadequate monitoring controls over the use of personal laptops and unencrypted portable storage devices.

Information Technology

Adequately established information technology controls help to protect sensitive information entrusted to the department. These controls include limited access to the University's computer systems, and restricting downloads of sensitive information. Another control is encryption software on equipment storing sensitive information. Ensuring employees have appropriate levels of system access helps prevent loss of vital University data and also prevents other abuses of the system.

We reviewed employee access levels for Oracle and verified that employees received appropriate level of access given their job responsibilities. We determined that all employees were granted the appropriate level of access to Oracle.

We inquired whether the department used portable storage devices such as external hard drives or thumb drives. We found that the department was using an unencrypted pin drive. We tested the device and found that no sensitive information was being stored. Unencrypted portable storage devices pose a significant risk to the University. Because this device was not encrypted, there is an increased risk of data loss.

Based on testing, we determined that the department had moderate controls over information technology.

CONCLUSION

Overall, we concluded that the department has a moderate system of financial and administrative controls. We identified areas where improvements could be made to internal controls. These controls include creating a policies and procedures manual; annually updating the risk assessment; ensuring that employees complete training and nepotism certifications; maintaining documentation on employee leave; monitoring the use of personal laptops and unencrypted portable storage devices.

Isabel Benavides CIA, CGAP, CFE
Director, Audits and Consulting Services

Khalil Abdullah CPA, CIA, CGAP
Internal Auditor I