November 11, 2014

Dr. Havídan 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 2014 Audit Plan, we completed a departmental audit of the Department of Communication. The objective of the audit was to evaluate the adequacy and effectiveness of the Department of Communication’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 FY 2013 (September 1, 2012 through August 31, 2013).

We performed audit procedures that included completion of an internal control questionnaire; interviews with staff; testing controls related to compliance with University policies and procedures; and performing substantive testing, on a sample basis, related to proper approvals of expenditures; time reporting; assets management; and segregation of duties.

Overall, we concluded that the Department of Communication had established a moderate system of financial and administrative internal controls in the areas evaluated. We identified areas where improvements to internal controls are necessary and management has agreed to take corrective action. 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
Chief Audit Executive
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>1</td>
</tr>
<tr>
<td>BACKGROUND</td>
<td>2</td>
</tr>
<tr>
<td>AUDIT OBJECTIVE</td>
<td>2</td>
</tr>
<tr>
<td>AUDIT SCOPE AND METHODOLOGY</td>
<td>2</td>
</tr>
<tr>
<td>AUDIT RESULTS</td>
<td>3</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>10</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

The Department of Communication (department) is an energetic multidisciplinary department made up of programs in Mass Communication, Communication Studies and Theatre/TV/Film. There are specialized career tracks within each program area. The department teaches both the theoretical and practical applications of the various fields of communication by offering a variety of classes and special projects and activities where students can get hands-on experience. The current chair assumed responsibility for the department in November 2011 as an interim chair.

As required by The University of Texas System’s (System) 1996 Action Plan to Enhance Internal Controls, an audit of departments should be performed every three (3) to five (5) years. 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, 2012 through August 31, 2013. 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:

- The policy and procedures manual was not comprehensive; it did not include guidance for performing procedures critical to running the department’s day-to-day operations. Additionally, an assessment of the department’s risks was not conducted;
- Not all required training and nepotism certifications were completed;
- The department did not use the ‘Leave Approval Request’ form to support employee leave;
- We were unable to locate a few fixed assets tested;
- Account reconciliation for one month was not completed;
- Lack of monitoring for personally owned laptops and unencrypted portable storage devices;
- The department stored sensitive information on unencrypted external hard drives.
BACKGROUND
The current chair assumed responsibility for the department in November 2011 as the interim chair, and was appointed chair in September 2012. The chair oversees 29 employees comprised of 23 faculty, and six (6) staff and was responsible for five (5) project accounts during FY 2013. A summary of the chair’s project account’s financial activity is summarized below.

<table>
<thead>
<tr>
<th>Project Account</th>
<th>Budget</th>
<th>Encumbrances</th>
<th>Actual</th>
<th>Funds Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>140COMU000</td>
<td>$1,759,035</td>
<td>$2,064</td>
<td>$1,750,681</td>
<td>$6,290</td>
</tr>
<tr>
<td>21COMU000</td>
<td>$867</td>
<td>$221</td>
<td>$202</td>
<td>$444</td>
</tr>
<tr>
<td>21COMU003</td>
<td>$72,499</td>
<td>$413</td>
<td>$56,046</td>
<td>$16,040</td>
</tr>
<tr>
<td>21THBO000</td>
<td>$36,911</td>
<td>$4,193</td>
<td>$18,407</td>
<td>$14,311</td>
</tr>
<tr>
<td>310THBO000</td>
<td>$96,331</td>
<td>$2,636</td>
<td>$89,962</td>
<td>$3,733</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>$1,965,643</strong></td>
<td><strong>$9,527</strong></td>
<td><strong>$1,915,298</strong></td>
<td><strong>$40,818</strong></td>
</tr>
</tbody>
</table>

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 2013 (September 1, 2012 through August 31, 2013). To accomplish the audit objective, we performed the following procedures:

- Interviewed the 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.
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.

We tested 20 employees for completion of annual trainings and nepotism certification. Additionally, we tested three (3) employees to determine whether an annual performance evaluation had been performed. The results of our tests are as follows:

- 9 out of 20 (45%) employees did not complete their sexual harassment training
- 10 out of 20 (50%) employees did not complete their annual standards of conduct training
- 12 out of 20 (60%) employees did not complete their information security training
- 16 out of 20 (80%) employees did not complete their annual nepotism certifications
- 3 out of 3 (100%) employees had an annual performance evaluation conducted.

We reviewed the department’s policies and procedures manual and determined that it was not comprehensive. For instance, it did not include procedures related to conducting account reconciliations, performing annual inventory, or documenting vacation and sick leave, to name a few. Additionally, we noted that the department had not completed a risk assessment.

Based on testing, we found that the department established an inadequate control conscious environment.
Recommendations:

1. The chair should develop a process to periodically verify whether faculty and staff have completed their required trainings.

Management Response:

1. The chair will develop a process to notify faculty and staff to complete their annual required trainings. Trainings will be included as an agenda item for discussion at each of the departmental employee meetings. In addition, the new online employee compliance education system will be used to help track staff and faculty training status. The chair’s process will include sending e-mail notifications to faculty and staff that have been identified as out of compliance to alert them that to reinforce the weekly notification from Compliance Support Services and recommend a date to complete the trainings. Completion of the required trainings will be included in the annual evaluations as merit points for service. The new, easier process for trainings has already resulted in a higher completion rate by faculty and staff. This policy will be outlined in the departmental policies and procedures manual.

Implementation Date:
November 1, 2014

2. The department chair should update the department’s policies and procedures manual to help guide employees in their day-to-day operations. This manual should include information such as employee training requirements, account reconciliation processes, funds handling procedures, annual inventory certification procedures, information on security controls, record retention requirements, and other relevant information.

Management Response:

2. The chair will begin to work with the faculty coordinators, the departmental supervisory staff and the Dean’s office to collate, identify and document the existing procedures and policies used by the department for its daily operations. The draft document will be subject to change as the new University departmental structure and HOP policies are created.

Implementation Date:
February 1, 2015
3. As part of our audit procedures, we identified areas of risk and assessed its impact and probability of occurrence and produced a risk assessment. The chair should utilize this document as a starting point towards developing a department risk assessment. This risk assessment should be evaluated annually and an action plan should be developed to mitigate high risks.

Management Response:

3. The risk assessment document created by the audit staff will be reviewed and edited as needed by the faculty and staff in the department. It will be incorporated into the departmental policies and procedures manual, distributed to faculty and staff and reevaluated on a regular basis.

Implementation Date:
September 1, 2014

Approval & Authorization

Adequately established approval and authorization controls help to ensure that expenditures are allowable and appropriate. During the audit period, the department chair was account manager for five (5) project accounts, with the administrative assistant II 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 2013.

Operating and Travel Expenditures

We judgmentally selected a sample of 22 operating and 11 travel transactions representing 45% and 43% 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 12 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 uses a ‘Leave Approval Request’ form to document employee leave. We tested two (2) employees’ vacation and sick leave for the months of November and December 2012. Based on our employee leave test, we determined that all employee timecards were approved by their supervisor; and that employee leave documentation agreed to the employee timecards. However, the department did not maintain all ‘Leave Approval Request’ forms in documenting all employee leave.

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

**Recommendation:**

4. The chair should ensure that all employee leave is supported by the ‘Leave Approval Request’ forms.

**Management Response:**

4. The Leave request forms for employees are now being filed in a common folder by the department administrative associate in addition to the employee’s files. Sick leave notifications received by email or text messages are being submitted for approval on the standard leave forms when the staff returns.

**Implementation Date:**

September 1, 2014

**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 20 assets with a historical cost greater than $1,000 to test for existence. We were unable to account for 3 out of the 20 (15%) assets, totaling $23,562. The assets were video cameras. 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.
Based on testing, we determined that the department established moderate safeguarding of fixed asset controls.

**Recommendation:**

5. The chair should ensure that the department’s inventory is monitored and tracked.

**Management Response:**

5. The chair is working with the staff and faculty involved in the areas to identify and remove outdated assets no longer needed by the programs. The removal of the clutter of old equipment will make it easier to track the current equipment that is in constant use by students and faculty in the department’s programs. The departmental equipment check out procedures for student use of equipment are being reevaluated and may be revised.

**Implementation Date:**

November 1, 2014

Additionally, we evaluated the department’s controls related with handling University funds. During FY 2013, the department handled funds (e.g. cash, checks). These funds were collected as a result of the Theatre Box Office activity. We reviewed the department’s procedures for safeguarding funds in accordance to the University’s funds handling policy HOP 8.6.6.

We selected a sample of 10 of the larger deposits from the account ledger to vouch the cash receipts to supporting documentation and to verify that the deposits were made timely. We determined that supporting documentation was available to substantiate the cash receipts and the deposits were made timely.

Based on testing, we determined that the department established adequate funds handling 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 revenue and funds handling, purchases, timecards, and statement of account reconciliations to evaluate segregation of duties.

The 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 II was responsible for preparing account reconciliations, while the department’s theatre business manager was responsible for cash handling activities, thereby keeping the custody of assets function separate from record keeping.

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

**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 and determined that the account reconciliations were performed and reviewed for the month’s tested. However, during this test, we discovered that the reconciliation for the month of June 2013 was never completed due to the retirement of an administrative support staff.

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

**Recommendation:**

6. The chair should ensure that all project accounts are reconciled and that timely project manager reviews are conducted.

**Management Response:**

6. The hire of a new administrative assistant II who came onboard in September 2013 has greatly improved the timely completion of the departmental reconciliations.

**Implementation Date:**

September 1, 2013

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.

**Recommendation:**

7. The chair should develop a procedure to identify individuals that utilize personal equipment to conduct University business. The chair should notify the Office of Privacy and Security about the use of these personally owned laptops, if any.

**Management Response:**

7. Faculty and staff have been notified to stop using unencrypted portable storage devices and have been encouraged to either use a remote connection or to store University related data to the OneDrive now available with IT’s deployment of Office 365. The chair will work with departmental employees to identify individuals that use personal laptops/desktops either on campus or at home for University business. The chair will also work with the CISO and administration staff to find out the level of the monitoring required for off campus equipment.

**Implementation Date:**
December 31, 2014

**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 the 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 several unencrypted external hard drives to back up electronic data. We tested three (3) of the drives and found that the devices
contained sensitive information. Unencrypted portable storage devices pose a significant risk to the University. Because these devices were not encrypted, there is an increased risk of critical data loss.

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

**Recommendation:**

8. The chair should work with the University’s Chief Information Security Officer to put into place adequate safeguards to secure sensitive information. In addition, the chair should ensure that sensitive information is only stored on encrypted drives.

**Management Response:**

8. The department now has a share drive available for use by the administrative staff. This has reduced the need to store departmental files on external drives. The external hard drives handed down from previous chairs with backups of departmental files and records have been replaced with approved encrypted drives. Previously the external hard drive was used to allow for the transfer of departmental files between faculty as the chair position reassigned. Past chairs used the external hard drives to store departmental files separately from their academic files on their desktops. Also these encrypted drives are used for the backup of the departmental computers as needed. Any other staff or faculty who have needed to back up departmental files from their office computers (such as the graduate coordinator) are being provided with approved encrypted drives. Currently the only files not on encrypted drives are archived departmental production photos.

**Implementation Date:**

September 1, 2014

**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 expanding the policies and procedures manual; developing a risk assessment; ensuring that employees complete training and nepotism certifications; maintaining documentation on employee leave; monitoring employees that utilize personal laptops and
unencrypted portable storage devices; and ensuring that sensitive information is stored on encrypted devices only.

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

Khalil Abdullah, CIA, CGAP
Internal Auditor I