Asset Management and Development

Change in Management Audit

Audit Report # 17-07
May 30, 2017

The University of Texas at El Paso
Institutional Audit Office

"Committed to Service, Independence and Quality"

THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

UTEP Institutional Audit Office
500 West University Ave.
El Paso, Texas 79968
915-747-5191
WWW.UTEP.EDU
WWW.UTSYSTEM.EDU

May 30, 2017

Dr. Diana Natalicio
President, The University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Natalicio:

The Office of Auditing and Consulting Services has completed a Change in Management audit of the Asset Management and Development Department. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in the audit report. The recommendations are intended to assist the department in strengthening controls and help ensure that the University's mission, goals and objectives are achieved.

We appreciate the cooperation and assistance provided by the Asset Management and Development Department during our audit.

Sincerely,

Lori Wertz
Chief Audit Executive

Report Distribution:

University of Texas at El Paso:
Mr. Richard Adauto III, Executive Vice President
Mr. Benjamin Gonzalez, Vice President, Asset Management and Development
Ms. Audrey Price, Assistant Vice President, Asset Management and Development
Ms. Sandra Vasquez, Assistant Vice President for Equal Opportunity (EO) and Compliance

University of Texas System (UT System):
System Audit Office

External:
Governor's Office of Budget, Planning and Policy
Legislative Budget Board
Internal Audit Coordinator, State Auditor's Office
Sunset Advisory Commission

Audit Committee Members:
Mr. David Lindau
Mr. Fernando Ortega
Mr. Steele Jones
Dr. Stephen Riter
Dr. Roberto Osegueda
Dr. Howard Daudistel
Dr. Gary Edens

Auditors Assigned to the Audit:
Mirna Naylor, Auditor
Cecilia Estrada Lozoya, Auditor
Victoria Morrison, IT Auditor

Table of Contents

EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services has completed a limited scope Change in Management Audit of the Asset Management and Development Department (AM&D). The audit scope was limited to selected financial and administrative activities for the period of January 1, 2016 through November 30, 2016. The objectives of this audit were to determine whether the Department is operating in a control conscious environment, verify that audited areas are in compliance with University policies and procedures and identify opportunities for improvement.

During the audit we noted the following:

- Based on auditor review of the Annual Giving & Database Systems Section, it was determined that there was awareness of Information Security Office policies, standards and guidelines. In addition, a review had been performed, and security incident management had been implemented.

- The department is in compliance with The University of Texas at El Paso's software standards, software purchasing procedures and license agreements.

- Six of eight laptop and desktop computers tested were not encrypted.

- Scheduled periodic review and monitoring is not performed on privilege administrative accounts and user accounts on servers, business systems, and shared drives. Additionally, a privilege administrative account on a server used by a vendor for support and problem resolutions has not been reviewed or monitored for security controls.

- Accounts for terminated employees are not reviewed to ensure timely removal.

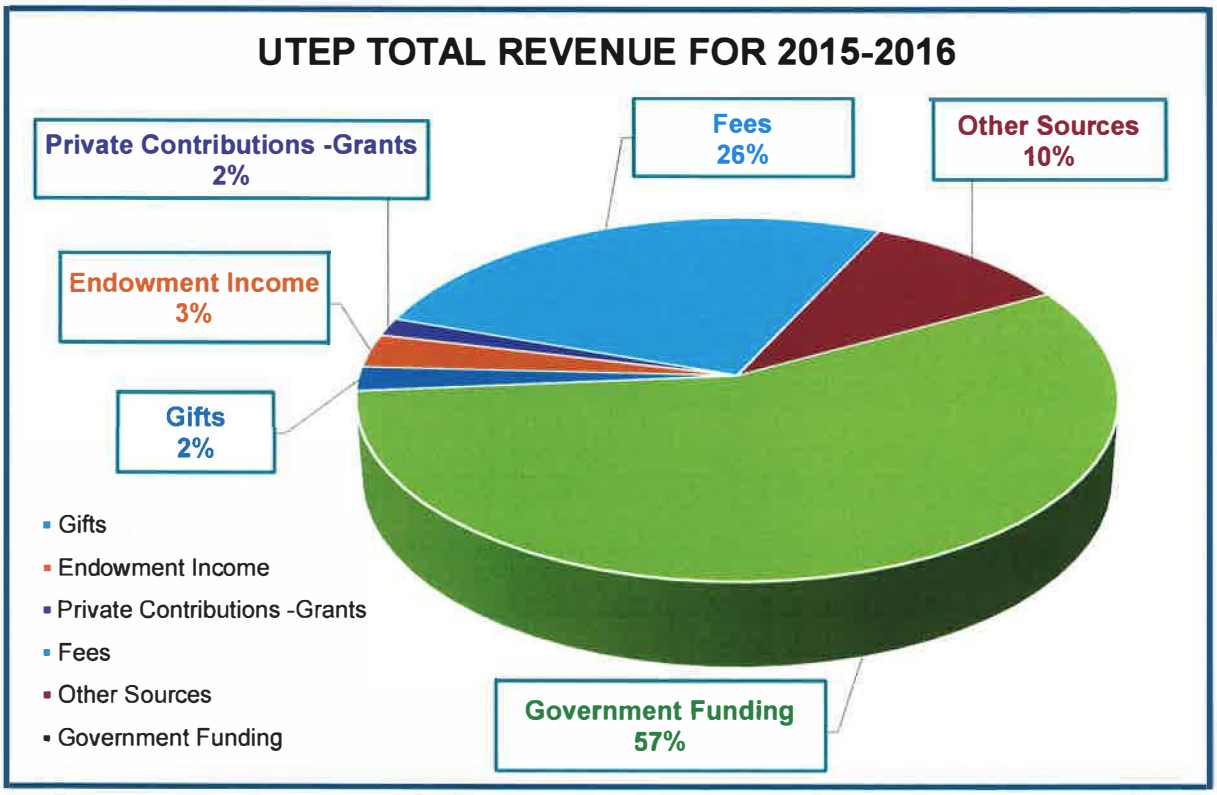
- AM&D did not send Fiscal Year 2016 Endowment Annual Reports to donors timely. In addition, some donors indicated that the information provided in the letters was not accurate.

- AM&D is not following university policy for the timely completion of account reconciliations.

- Many areas of AM&D lack written policies and procedures for the job functions they perform.

BACKGROUND

The University of Texas at El Paso (UTEP) encourages donor contributions from alumni and community leaders to provide financial support to attract excellent faculty, invest in specialized programs and facilities, and provide students with scholarships and the necessary research tools and skills to provide opportunities for groundbreaking research advancements. As state funding for higher education decreases, private donations to support student success and research initiatives are critical to the achievement of our goal of becoming a Tier One university.



AUDIT OBJECTIVES

The objectives of this audit were to determine if:

A. the department is functioning in a control conscious environment,

B. Asset Management and Development (AM&D) is in compliance with The University of Texas System (UT System) and The University of Texas at El Paso (UTEP) policies regarding the gift and endowment processing,

C. administrative and financial operations are performed in accordance with University policies and procedures, and

D. security controls and safeguarding of information and resources are in place.

SCOPE AND METHODOLOGY

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors.

Audit procedures included performing a risk analysis, reviewing departmental policies and procedures, interviewing personnel, reviewing significant accounts, assessing gift and endowment processing procedures, as well as the account reconciliation process. Limited testing was performed in the areas of maintenance and operations and ProCard expenditures, and IT security and safeguards were reviewed to verify the effectiveness of internal controls and compliance with the University's administrative and financial policies and procedures. The scope of the audit was January 1, 2016 through November 30, 2016.

RANKING CRITERIA

All findings in this report are ranked based on an assessment of applicable qualitative, operational control and quantitative risk factors, as well as the probability of a negative outcome occurring if the risk is not adequately mitigated. The criteria for the rankings are as follows:

Priority – An issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.

High – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

Medium – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

Low – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

AUDIT RESULTS

A. IT Security Controls and Safeguarding of Information

A.1 Information Security Control Awareness

We interviewed the Director of the Annual Giving & Database Systems Section and conducted testing to determine whether:

- there was awareness of the Information Security Office policies, standards, and guidelines,
- a review had been performed by the Information Security Office, and
- security incident management had been implemented.

No exceptions were noted.

A.2 Application-Software Management

The department is in compliance with UTEP'S software standards, software purchasing procedures and license agreements. In addition, current versions of the business application systems are in use and change management procedures are directed by Enterprise Computing (EC). The Annual Giving & Database Systems section is aware of the department's information resources as documented in the Office of Auditing and Consulting Services, IT Assessment Information Resource worksheet.

No exceptions were noted.

A.3 Encryption of computers

In accordance with *UT System UTS 165 Information Resources Use and Security Policy,* "*all University of Texas at El Paso (UTEP) laptops, desktops, and mobile devices were to be encrypted, by August 2012, to reduce the risk to exposure of confidential information.*"

A judgmental sample of eight computers was tested for safeguards and security, such as encryption and antivirus, to reduce the risk of compromised information or malicious threats. Six of eight computers were not encrypted. In addition, one computer had outdated and inactive antivirus software, which was corrected prior to the end of the audit.

There is no verification performed to ensure all computers in the department are encrypted, which could result in a possible loss of data and threats to the system.

Recommendation:

Request a complete review of AM&D's computing devices by Technical Support. Implement, in all laptop and desktop computers, necessary safeguards such as encryption and antivirus to reduce the risk of compromised information or malicious threats. Obtain exemptions as needed from the Information Security Office and document all computers not encrypted.

Level: This finding is considered **High** risk due to the possibility of compromised information or malicious threats.

Management Response:

A complete review of AM&D's computing devices by Technical Support will be undertaken. Through this review, we will ensure that all laptop and desktop computers have all necessary safeguards, such as encryption and antivirus software, to reduce the risk of compromising information or being adversely affected by malicious threats. We will obtain exemptions as needed from the Information Security Office and document all computers that are not encrypted.

Responsible Party:

Christine Pineda, Director of Advancement Services

Implementation Date:

August 31, 2017

A.4 Privilege Administrative Accounts

In accordance with *UTS Policy 165 Information Resources Use and Security, Section 8 Administrative/Special Access*:

> *"All Entities shall adopt special procedures that ensure all administrative/special access accounts with elevated access privileges on computers, network devices, or other critical equipment (example: accounts used by system administrators and network managers) shall be used only for their intended administrative purpose and that all authorized Users must be made aware of the responsibilities associated with the use of privileged special access accounts.*
>
> *These procedures must address:*
>
> *8.1 acceptable use of administrative/special access accounts and intended administrative purposes;*

8.2 authorizing use of administrative/special access accounts;

8.3 reviewing, removing, and/or disabling administrative/special access accounts at least annually, or more often if warranted by risk, to reflect current authorized User needs or changes on authorized User role or employment status; and

8.4 escrowing login passwords for each secured system for access during emergencies. Individual User login passwords shall not be escrowed.

Two privilege administrative accounts for people no longer employed at the University were found. These accounts were removed during the audit.

We also found a privilege administrative account on a server which is used by the vendor for problem resolution of a business system. The account was enabled and had no expiration date, increasing the risk of unauthorized access and possible intrusion. The IT auditor notified EC and the Chief Security Officer and the account was disabled. An alternate solution will be found by reviewing and implementing security controls.

Recommendation:

A scheduled periodic review and monitoring of privilege administrative account(s) should be performed, to include administrative rights by a vendor to support and provide problem resolution of a business system. The privilege administrative account should be enabled only when needed and contain an expiration date. Additionally, the password should be changed at least once a year and logins should be monitored and reviewed.

Level: This finding is considered **High**, due to the risk of unauthorized access and intrusion to UTEP information resources.

Management Response:

A scheduled periodic review and monitoring of privileged administrative account(s) will be performed, to include a review of administrative rights by vendors who support and provide problem resolution of our business systems. Vendors requiring access to campus servers will notify the Director of Database Systems and provide specific timeframes the server will need to be accessed. EC will be notified and provided with timeframes the vendor requires. EC sets up automatic expiration times to lock servers. The Director of Database Systems will communicate with EC to monitor expiration dates to any special privileged accounts to department servers (after specific accessed times) and on a yearly basis.

Responsible Party:

Erika Villegas, Director of Database Systems

Implementation Date:

Effective immediately and Quarterly reviews beginning July 1, 2017

A.5 Access Management Monitoring and Control

In accordance with Information Security Office, *UTEP Information Security Policies, Account Management, 4.0 Policy*:

> *"… Data Owners, System Owners, System Administrators and/or other authorized personnel:*
>
> - *are responsible for removing the accounts of individuals that change roles within the University or are separated from their relationship with UTEP*
> - *must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes*
> - *must have a documented process for periodically reviewing existing accounts for validity*
> - *are subject to independent audit review*
> - *must provide a list of accounts for the systems they administer when requested by the Information Security Office…"*

The IT Auditor tested access management controls in AM&D business systems and file servers (shared drives). Sixteen accounts with access to the department share drive and one account with access to a business system were identified as active or enabled for terminated employees. The business owner disabled and/or requested the removal of these accounts during the audit.

Accounts for terminated employees are not reviewed to ensure timely removal, increasing the risk of unauthorized access to UTEP Information Resources.

Recommendation:

A scheduled periodic review and monitoring of user accounts should be performed and all unauthorized users should be removed.

Level: This finding is considered **Medium** risk, due to possible unauthorized access to UTEP information resources.

Management Response:

A scheduled periodic review and monitoring of user accounts will be performed and all unauthorized users will be removed.

Responsible Party:

Christine Pineda, Director of Advancement Services

Implementation Date:

August 31, 2017

B. Compliance with gift and endowment policies

B.1 Annual Reports to Endowment Donors

UTS 117 Endowment Compliance Plan Systemwide Standards and Guidelines, Section 4.4 states:

"Annual Reports to Endowment Donor(s). The U. T. System institution and U. T. System Administration should provide annual reports to the donor(s) of each endowment. The report should summarize the major activities associated with the endowment, include a financial statement for the endowment for the report period and, when appropriate, provide information on the holder(s) or the recipient(s) of the endowment."

AM&D did not send Endowment Annual Reports to donors timely. In addition, some donors indicated that the information provided in the letters was not accurate. The lack of policies and procedures for the review of donor reports leads to errors and inconsistencies and may increase the possibility of losing critical contributions for education and research.

Recommendation:

To ensure timely and accurate reports to donors,

- *Policies and procedures, including time frames for the delivery of Annual Reports to Donors should be developed.*

- *A schedule should be developed to assist with the process, and shared with all personnel involved.*
- *The reports should go through a structured review process prior to distribution to ensure all information is complete and accurate.*
- *The tracking log of reports should indicate the date sent to donors.*

Level: This finding is considered **Medium** risk, due to the possibility of losing critical contributions for education and research.

Management Response:

Will develop policies and procedures, including time frames for the delivery of Annual Reports to Donors. Timeline for reporting process will be shared with all personnel involved in this activity and reports will undergo a structured review process prior to distribution to ensure all information is complete and accurate. A tracking log of this annual mailing will be implemented indicating date and type of report mailed to donor.

Responsible Party:

Christine Pineda, Director of Advancement Services

Implementation Date:

October 10, 2017

C. Administrative and Fiscal Operations

C.1 Cost Center Reconciliation

The UTEP Handbook of Operating Procedures (HOP) Section VII, Chapter 5 Cost Center/Project Review states:

"In accordance with UTS 142.1, all cost center/project administrators are required to review the cost center/project for which they have signature authority on a monthly basis.... Discrepancies should be resolved within 60 days after their identification.... Both the reviewer and approver must sign off on the reconciliation. Documentation should be retained and kept available to serve as back up for charges made on departmental accounts." In addition, account reconciliations can identify errors and potential fraudulent activities on a timely basis."

AM&D is not following university policy for the timely completion of account reconciliations. Reconciliations of cost center and project accounts are performed quarterly and are not approved by the department owner. If reconciliations are not performed timely and properly approved, errors and fraud may be undetected.

Recommendations:

Account reconciliations should be prepared on a monthly basis. Both the reviewer and approver must sign off on the reconciliation, and documentation should be retained to serve as back-up for charges made on department accounts. An in-depth analysis of all Asset Management and Development accounts should be performed to identify inactive accounts and investigate the reasons for inactivity and unexpended balances.

Level: This finding is considered **Medium** risk, due to the possibility that errors and fraud may not be detected and corrected in a timely manner.

Management Response:

Monthly Account reconciliations for current fiscal year will be prepared. Both the reviewer and approver will evaluate and certify the monthly reconciliation, in writing, and documentation will be retained to serve as support for charges made to department accounts. An in-depth analysis of all Asset Management and Development accounts will be performed to identify inactive accounts and investigate and document the reasons for inactivity and unexpended balances.

Responsible Party:

Christine Pineda, Director of Advancement Services

Implementation Date:

August 31, 2017

C.2 Policies and Procedures

Many areas of AM&D lack written policies and procedures for the job functions they perform. Daily operations may not be carried out on a timely basis, and there is a higher risk of costly mistakes due to lack of clear guidance, as policies and procedures identify key activities and provide a plan of action to carry out organizational operations. These policies must be consistent with all applicable laws, regulations, policies and procedures.

***Recommendation**:*

Policies and procedures should be updated to reflect the administrative, financial and information technology operations of the department in order to provide guidance to employees and facilitate oversight and monitoring.

Level: This finding is considered **Medium** risk due to the risk that daily operations could not be carried out on a timely basis, and the possibility of costly mistakes due to lack of clear guidance.

Management Response:

Policies and procedures will be updated to reflect the administrative, financial and information technology operations of the department in order to provide guidance to employees and facilitate oversight and monitoring.

Responsible Party:

Audrey Price, Assistant VP for Asset Management and Development

Implementation Date:

December 31, 2017

C.3 Additional Observations

Additional observations noted and discussed with management include:

- Inaccurate inventory tracking
- Missing Keys
- Lack of appropriate support documentation for expenditures
- Lack of mission and vision statement to align with university goals

CONCLUSION

During the audit, weaknesses were identified which we believe can be strengthened by implementing the recommendations detailed in this report.

We wish to thank the Asset Management and Development Department for the assistance and cooperation provided throughout the audit.