Departmental Change in Management Audits Fiscal Year 2012

November 2012

The University of Texas at Austin
Office of Internal Audits
UTA 2.302
471-7117
The University of Texas at Austin
Internal Audit Committee

Mr. William C. Powers Jr., Chair, President
Dr. Steven W. Leslie, Executive Vice President and Provost
Mr. Kevin P. Hegarty, Vice President and Chief Financial Officer
Dr. Patricia L. Clubb, Vice President for University Operations
Ms. Patricia C. Ohlendorf, Vice President for Legal Affairs
Dr. Juan M. Sanchez, Vice President for Research
Dr. Gage E. Paine, Vice President for Student Affairs
Dr. Charles A. Roeckle, Deputy to the President
Ms. Mary E. Knight, CPA, Associate Vice President and Budget Director
Mr. Frank W. Maresh, CPA, External Member
Mr. Rudolph H. Green, Director, University Compliance Services
Mr. Cameron D. Beasley, University Information Security Officer
Mr. Michael W. Vandervort, Director, Office of Internal Audits

The University of Texas at Austin
Office of Internal Audits

Director: Michael Vandervort, CPA
Assistant Directors:
*Kathey Mitchell, CIA, CGAP
Chris Taylor, CIA, CISA
Auditor IV: William Koenig, CIA, CFE, CGAP
Auditor III: *Brenda Guerrero
Auditor II: *Andrew Keegan
Auditor I: Ashley Foster
*S Caroline Poquez
Cameosha Jones
Sr. IT Auditor: Tod Maxwell, CISA, CISSP
IT Auditor: Brandon Morales, CISA, CGAP

* denotes project members

This report has been distributed to Internal Audit Committee members, the Legislative
Budget Board, the State Auditor's Office, the Sunset Advisory Commission, the
Governor's Office of Budget and Planning, and The University of Texas System Audit
Office for distribution to the Audit, Compliance, and Management Review Committee of
the Board of Regents.

Departmental Change in Management Audits
Project Number 779.12
November 27, 2012

President William C. Powers, Jr.
The University of Texas at Austin
Office of the President
P.O. Box T
Austin, Texas 78713

Dear President Powers,

We are in the process of completing the Change in Management Audit. Our scope included 16 units selected based on a risk assessment and changes in departmental management as part of our Fiscal Year 2012 Audit Plan. Our audit process included surveying department heads by questionnaire, interviewing management and staff in each unit, reviewing electronic office structures, and transaction testing.

Eight reports have been issued thus far. Due to the individual nature of each review, we have attached the following reports for your information:

4620-000  Texas Student Media
2631-000  Center for Information Assurance and Security
3550-000  Professional Development Center
0055-000  Dell Pediatric Research Institute
3900-000  Tarlton Law Library
6130-000  University of Texas Press
4035-000  University of Texas Elementary School
5010-000  University Development Office

We appreciated the cooperation and assistance of all University personnel involved in this review and hope that the information presented herein is beneficial.

Sincerely,

Michael W. Vandervort, CPA
Director

cc: Internal Audit Committee Members
MEMORANDUM

To: Mr. David Hamrick, Director
   University of Texas Press

From: Mr. Michael Vandervort, CPA
       Director

Subject: Final Report – Change in Management Audit, Fiscal Year 2012
         Unit #6130-000: University of Texas Press (UT Press)

Date: September 7, 2012

We have completed our audit of your compliance with and awareness of certain
University of Texas at Austin (UT Austin) policies and procedures.

We reviewed internal controls in the following areas:

- Electronic Office Structure
- General Departmental Information/Organization/Activities
- Account Reconciliation
- Outside Employment/Conflict of Interest
- Cash and Cash Equivalent Handling
- Accounts Receivable
- Petty Cash
- Merchandise for Resale
- Inventory
- Purchasing Activities
- Procurement Cards
- Travel Expenditures
- Entertainment and Official Occasion Expenditures
- Authorization for Individual Services
- Contracts
- Time Reporting
- Information System Security
- Endowments

We performed the following procedures to complete this audit:

- Reviewed your electronic office structure;
- Tested account certifications, entertainment and official occasion transactions,
  endowments, annual physical inventory completion, employees’ appointment
  statuses, and information system security;
- Surveyed via questionnaire to ascertain your reported strength in internal controls
  and compliance with UT Austin rules; and
- Clarified follow-up issues with you and your staff.
This audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and with *Government Auditing Standards*.

Based on the above procedures, UT Press appears to have reasonable to strong controls in most areas. Seven opportunities for improvement were noted.

**Information System Security – Management of Sensitive Digital Data**

The unit does not follow UT Austin’s Records Retention Schedule for disposal of digital data containing Category I data. Without disposing digital data according to the records retention schedule, there may be increased risk of unauthorized access to the unit’s data.

Section 5.11.4.2 of UT Austin’s *Information Resources Use and Security Policy* states that “the university shall discard electronic media (for example, disks, tapes, hard drives, etc.) containing Category I-Data in accordance with university’s records retention schedule.”

**Recommendation 1:** UT Press management should ensure that the unit follows UT Austin’s Records Retention Schedule for disposal of digital data.

**Management Response:** UT Press disposes of digital data stored on disks and tapes by physically shredding the media. We dispose of Windows-based computer hard disks by sending them to Flawn Academic Center Hard Disk Destruction service. For Apple computer-based hard disks, we use the Disk Erase Utility and erases and writes random data 7 times. The machine, with disk installed, is then sent to surplus. This has been our policy for many years.

In addition, the IT manager will review the digital data disposition needs on a monthly basis, send an email regarding records retention to staff, and dispose properly of any items within 30 days.

**Implementation Date:** Implemented (an email to staff was sent in mid-May 2012)

**Information System Security – Administrative Access**

Computers are configured to allow users to operate with administrative rights. It may be difficult to protect against unauthorized access to data, software installations, and system configuration changes to workstations when users operate with administrative rights.

Section 5.4 of UT Austin’s *Information Resources Use and Security Policy* states that, “accounts with elevated access privileges on computers, network devices, or other critical equipment shall be used only for their intended administrative purposes and that all authorized Users must be made aware of the responsibilities associated with the use of privileged special access accounts.”
**Recommendation 2:** UT Press management should ensure that users operate workstations with the least privileges necessary to conduct business related functions.

**Management Response:** UT Press IT staff is evaluating the level of access privileges necessary for each employee and will write a policy that assigns either administrator access or standard access depending on that employee's functions.

**Implementation Date:** Implemented (May 15, 2012).

**Information System Security – Backup Recovery of Systems and Data**
Backup server tapes are stored in a closet in the same location as the server. The unit may not be able to recover data if both the server and its backup tapes are in the same location when an unexpected event(s) such as natural disaster, fire, and/or theft occurs.

Section 5.5.2.3 of UT Austin’s *Information Resources Use and Security Policy* states that, “each college, school, or unit responsible for a system(s) should maintain a disaster recovery plan. The recovery plan includes requirements for off-site storage needs.”

**Recommendation 3:** UT Press management should designate a secure storage location in a separate building approved by the Information Security Office.

**Management Response:** UT Press will either switch to UT Backup automatic backup system or move storage location to a separate building.

**Implementation Date:** Implemented (May 15, 2012).

**Information System Security – Physical Access**
The server, which stores the entire unit’s data, is located in a shared office, protected with only a traditional lock and key. As a result, there may be unauthorized access to UT Austin information stored on the server.

Section 5.19.2.2 of UT Austin’s *Information Resource Use and Security Policy* states that “all facilities supporting information resources must have physical access controls in proportion to the importance, sensitivity, and accountability requirements of the data and the systems housed in that facility.”

**Recommendation 4:** UT Press management should ensure that the server is physically secured behind a locked door with a locking mechanism such as a Building Access Control System or Locknetics style device and is accessible only to UT Press IT employees.

**Management Response:** UT Press will install one of the recommended options listed above.
Implementation Date: Implemented (July 12, 2012).

Information System Security – Securing Unattended Devices
Password-protected screensavers are not prompted on computers. Unauthorized access to unattended devices may result in harmful or fraudulent disclosure, modification, or deletion of sensitive electronic data. In addition, it may lead to the misuse of critical applications or email accounts.

Section 5.18.5 of UT Austin’s Information Resource Use and Security Policy states that, “unattended computing devices must be secured from unauthorized access. Logical security options include screen saver passwords and automatic session time-outs.”

Industry best practice encourages that password-protected screensavers activate after 15 minutes of idle time.

Recommendation 5: UT Press management should ensure that all computers enable the password-protected screensaver setting that activates after 15 minutes of inactivity.

Management Response: UT Press will make this change.

Implementation Date: Implemented (May 1, 2012).

Information System Security – Account Management
According to IT Management, all computers are not centrally-managed and are configured with local user accounts. The IT Manager creates user’s passwords without following UT Austin’s password requirements. In addition, users can change their log-on password without the IT Manager’s knowledge. However, users cannot gain access to files on the file server unless the IT Manager resets their password. Without following the UT Austin’s password requirements, unauthorized individuals can make harmful or fraudulent disclosure, modification, or deletion of UT Austin’s data.

Sections 5.3.1-3 of UT Austin’s Information Resources Use and Security Policy state that, “proper management and use of computer accounts are basic requirements for protecting the university’s information resources. All offices that create access accounts for applications, networks, or systems are required to manage the accounts in accordance with the university’s access management processes. Access to an information resource may not be granted by another user without the permission of the owner or the owner’s delegated custodian of the information resource. All accounts are to be created and managed using the following required account management practices:

- All accounts that access non-public university information resources must follow an account creation process. This process shall document who is associated with the account, the purpose for which the account was created, and who approved the creation of the account. All accounts wishing to access the university’s non-public information resources must have the approval of the owner of those resources. These measures also apply to account created by/for use of outside vendors or contractors.
Each account having special privileges must adhere to the university’s password requirements.

All accounts must be able to be associated with an identifiable individual or group of individuals that are authorized to use that account (for example, the UT-EID).

**Recommendation 6:** UT Press management should create a more centrally-managed computing environment that ensures UT Austin owned computers are added to UT Austin Active Directory, which forces users to create strong passwords.

**Management Response:** UT Press will create a centrally-managed computing environment connected to the Austin Active Directory. UT Press is unsure of how switching to Austin Active Directory will affect our use of critical proprietary software (Cat’s Pajamas). The IT Manager has scheduled a consultation on August 10 with ITS staff to determine how best to proceed.

**Implementation Date:** If we are able to implement a change without adversely affecting our proprietary software, we will make that change by October 15, 2012.

**Information System Security – Software Licensing**

The unit does not track the software that is installed on computers. Without logging all software on all UT Austin owned devices, software may be installed on to computers without the proper license.

Section 5.24 of UT Austin’s *Information Resources Use and Security Policy* states that “all software used on university computers will be used in accordance with the applicable software license. Unauthorized or unlicensed use of software is regarded as a serious violation subject to disciplinary action and any such use is without the consent of the university.”

**Recommendation 7:** UT Press management should ensure that the appropriate number of software licenses in use are accounted for.

**Management Response:** UT Press is enhancing its database of computer assets to include specific software installed on each machine and to indicate license information.

**Implementation Date:** Implemented (June 1, 2012).

Attached you will find a Change in Management Report Card, which is based on our understanding of the controls in place in your unit at the time of our review. If fully implemented, the recommendations above would improve your overall evaluation.
We appreciate the assistance and cooperation of you and your staff in this audit and hope that the information presented herein is beneficial. If you have any questions, please contact Caroline Poquez at caroline@austin.utexas.edu or 471-9837.

MV: cp

Attachment

cc:  Dr. Steven Leslie, Executive Vice President and Provost  
     Dr. Charles A. Roecke, Deputy to the President
<table>
<thead>
<tr>
<th>Areas Reviewed</th>
<th>Reasonable to Strong Controls in Place</th>
<th>Opportunity for Improvements</th>
<th>Significant Deficiencies</th>
<th>Material Weaknesses¹</th>
<th>Not Applicable to the Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Office Structure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Departmental</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information/Organization/Activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Reconciliation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endowed Positions/Gift Administration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outside Employment/Conflict of Interest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash Registers/Cashiers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cash and Cash Equivalent Handling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounts Receivable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Petty Cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Merchandise for Resale</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inventory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controlled Items</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchasing Activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procurement Cards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Travel Expenditures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entertainment and Official</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occasion Expenditures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authorization for Individual Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contracts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information System Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹ A weakness that significantly impacts the UT Austin’s operations or finances