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. Clabb, 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
               *Caroline Poquez
Sr. IT Auditor: Cameosha Jones
IT Auditor: Tod Maxwell, CISA, CISSP
               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: Ms. Melissa Chavez, Executive Director  
The University of Texas Elementary School

From: Mr. Michael Vandervort, CPA  
Director

Subject: Final Report – Change in Management Audit, Fiscal Year 2012  
Unit #4035-000: The University of Texas Elementary School (UT Elementary School)

Date: September 21, 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,
- Endowed/Gift Administration,
- Outside Employment/Conflict of Interest,
- Cash and Cash Equivalent Handling,
- Accounts Receivable,
- Petty Cash,
- Inventory,
- Purchasing Activities,
- Procurement Cards,
- Travel Expenditures,
- Entertainment and Official Occasion Expenditures,
- Authorization for Individual Services,
- Contracts,
- Time Reporting, and
- Information System Security.

We performed the following procedures to complete this audit:

- Reviewed your electronic office structure;
- Tested account certifications, entertainment and official occasion transactions, annual physical inventory completion, employees’ appointment statuses, and information system security;
- Surveyed via a 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 Elementary School appears to have reasonable to strong controls in most areas. Eight opportunities for improvement are noted.

**Cash and Cash Equivalent Handling**

The transfer of funds between employees is not documented. Without proper documentation of their transfer, there is limited accountability regarding the custody of funds.

Section 6.1.C.3 of UT Austin’s Handbook of Business Procedures states that, “every time funds are transferred, the funds should be counted in the presence of both parties” and that this transfer should be documented with signatures from both individuals.

<table>
<thead>
<tr>
<th>Recommendation 1:</th>
<th>Management should ensure that every time funds are transferred between employees, the funds are counted and the transfer is documented with signatures from both individuals.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Management Response:</th>
<th>The teacher handbook has written procedures that are expected to be followed by teachers and the business office. The relevant section of the handbook has been updated to the following:</th>
</tr>
</thead>
</table>

*Money collected for purposes such as field trips or fundraisers should be turned into the business office by noon in the Teacher Money Envelope. Include the deposit slip in the envelope and enter the total payment amount on the front. The office will not accept any money unless it is in teacher money envelope, and the payment is logged on the outside of that envelope and the deposit slip is filled out and signed by the collecting teacher. Please fill out the front of the envelope accurately and completely. Both the business office and the teacher should count the money together at this time.* [Emphasis added] A confirmation receipt will be attached to the copy of the deposit slip and returned to you indicating receipt of money. Each grade level will share a receipt book and if $5.00 or more dollars are collected a receipt must be written to the parent/guardian. If it is less than $5.00 teachers must keep a log of the students to show who has turned in money.

| Implementation Date: | Implemented 8/23/12. |

**Information Systems Security - Backup Recovery of Systems and Data**

The file server is not backed up on a regular basis. Without a regular backup of systems and data, it would not be possible to recover information if it was deleted or destroyed in an unexpected event such as natural disaster, fire, and/or theft.
Section 5.5.1 of UT Austin’s Information Resources Use and Security Policy states that “All university data, including data associated with research, must be backed up in accordance with risk management decisions implemented by the Data Owner.”

**Recommendation 2:** Management should create and implement a plan to regularly backup computer systems and data.

**Management Response:** The University of Texas Elementary school will purchase Austin Disk by the end of September 2012. We will be purchasing 500 gigabytes to cover the size of the server ($1,400). Region 13 backs up all of our student records through a program called TxEIS. This is a web based program. The student records are backed up at the Region 13 service center. The program cost the school $ 9,000 per year.

**Implementation Date:** September 30, 2012

**Information Systems Security - Physical Access to Servers**
Non-IT individuals have physical access to the UT Elementary server. Without adequately securing the server room, there is an increased risk of unauthorized access to UT Austin’s information stored on the server.

According to Rule 5.19.2 of UT Austin’s Information Resources Use and Security Policy, “all facilities supporting information resources must have physical access controls in proportion to the importance, sensitivity, and accountability requirements of the data and systems housed in that facility.”

**Recommendation 3:** Management should ensure that physical access to the server is limited to IT personnel and that the physical access controls are in proportion to the importance, sensitivity, and accountability requirements of the data and systems.

**Management Response:** The University of Texas Elementary School’s new administration building has an MDF closet that houses the server with restrictive access using the BAC system. ITS and Eric Johnson [Senior Desktop Support Specialist] have access to this MDF closet. UT Elementary moved into the new building on June 8, 2012.

**Implementation Date:** Implemented 6/8/12.

**Information Systems Security - Disaster Recovery Plan (DRP)**
A DRP has not been created. Without a documented DRP in place, UT Elementary School administrators may not be able to adequately recover critical systems and data in the event of a disaster.

According to Rule 5.5.2 of UT Austin’s Information Resources Use and Security Policy, “each college, school, or unit responsible for a system(s) should maintain a disaster recovery plan.” The recovery plan should include the following:
• Procedures for recovering data and applications in case an unexpected event occurs such as a natural disaster, power or system disk failure, espionage, data entry error, human error, or other systems operation errors;
• Assignments of operational responsibility for backup of all systems connected to the respective network;
• Requirements for off-site storage needs;
• Physical and network access controls for on-site and off-site storage; and
• Processes to ensure backups are viable and can be recovered.

**Recommendation 4:** Management should ensure that a comprehensive documented DRP exists within UT Austin’s Restarting Texas DRP application¹. This plan should be reviewed and updated as necessary and tested annually.

**Management Response:** The University of Texas Elementary School will use UT Austin’s Restarting Texas DRP application to create their own disaster recovery plan. We will have a plan in place by the end of this school year.

**Implementation Date:** May 2013

**Information Systems Security - Compliance Training**
Four out of 18 employees had not completed TX Class CW 170 – IT Security Awareness. There is an increased risk of security incidents if employees are not properly trained regarding the use of department information resources.

According to Rule 5.22 of the UT Austin Information Resources Use and Security Policy, all employees are required to take compliance training within the first 30 days of employment and every two years thereafter.

**Recommendation 5:** Management should ensure that all employees complete TX Class CW 170 – IT Security Awareness within the first 30 days of employment and every two years thereafter.

**Management Response:** Melissa M. Chavez, Executive Director, has asked all employees to complete the TX Class CW 170 – IT Security Awareness online class by the end of this month.

**Implementation Date:** October 1, 2012

**Information Systems Security - Position of Special Trust Forms**
Positions with access to Category I data have not been designated as such in the Human Resource Management System. As a result, employees in those positions have not completed Position of Special Trust forms. If the form is not completed, employees may

---

¹ Restarting Texas is an application provided by the Information Security Office and is designed for departmental disaster recovery planning.
not be aware of their responsibilities for handling Category I data. This could lead to a loss or misuse of the data.

The Office of the Chief Information Officer’s (CIO) website states that:

“all university employees with elevated systems privileges and access to Category I university data shall be required to acknowledge annually the additional responsibilities they bear with those privileges by signing a Position of Special Trust form. Supervisors are expected to review the current job duties to determine if designation of Position of Special Trust is appropriate.”

**Recommendation 6:** Management should ensure that all positions with access to Category I data are designated as such in the Human Resource Management System. All individuals in those positions should complete a Position of Special Trust form.

**Management Response:** Julie Nance [Business Manager] will work with HR to ensure that the [HRMS] system [indicates which of] our employees have access to Category I data AND that the required “Position of Special Trust” form is filled out and kept in our records.

**Implementation Date:** September 30, 2012

**Information Systems Security - Administrative Access**
Employees have administrative privileges added to their user accounts when a laptop is checked out for an extended time. When users operate with administrative privileges at all times, it is difficult to protect against unauthorized access to data, software installations, and system configuration changes to workstations.

According to Rule 5.4.1 of UT Austin’s Information Resources Use and Security Policy, “individuals who use accounts with special privileges (for example, System Administrators) must use these accounts only for their intended administrative purposes.”

**Recommendation 7:** Management should ensure that administrative rights are not added to employees’ user accounts. A new user account, with administrative privileges, should be created and used instead.

**Management Response:** Eric Johnson [Senior Desktop Support Specialist] has created a local admin account for users to administer their computers off site.

**Implementation Date:** Implemented 8/23/12.

**Information Systems Security - Securing Unattended Devices**
All five computers tested did not have the password-protected screen saver settings enabled. Unauthorized access to unattended devices can result in harmful or fraudulent
disclosure, modification, or deletion of electronic data. In addition, it may lead to the misuse of critical applications or email accounts.

According to Rule 5.18.5 of UT Austin’s Information Resources Use and Security Policy, unattended computing devices must be secured from unauthorized access. Logical security options include screensaver passwords and automatic session time-outs.

**Recommendation 8:** Management should ensure that all computers are configured with password protected screen savers that activate after 15 minutes of idle time.

**Management Response:** Eric Johnson [Senior Desktop Support Specialist] will create a group policy for Windows Austin domain today that will create a 15 minute password protected screen saver for all office staff computers.

**Implementation Date:** Implemented 8/23/12.

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 Andrew Keegan at 471-9836 or andrew.keegan@austin.utexas.edu.

MV: ak

Attachment

cc: Mr. Gregory J. Vincent, Vice President for Diversity and Community Engagement
Dr. Charles A. Roecke, Deputy to the President
### Change in Management Report Card
**UT Elementary School, Unit # 4035-000**

<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 Weaknesses&lt;sup&gt;2&lt;/sup&gt;</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 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 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>

---

<sup>2</sup> A weakness that significantly impacts the UT Austin’s operations or finances