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. Roockle, 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
              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,

[Signature]
Michael W. Vandervort, CPA
Director

cc: Internal Audit Committee Members
MEMORANDUM

To: Dr. Linda Hicke, Dean  
   College of Natural Sciences

From: Mr. Michael Vandervort, CPA  
       Director

Subject: Final Report – Change in Management Audit, Fiscal Year 2012  
         Unit #0055-000: Dell Pediatric Research Institute (DPRI)

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,
- Inventory,
- Controlled Items,
- Purchasing Activities,
- Procurement Cards,
- Travel Expenditures,
- Entertainment and Official Occasion Expenditures,
- 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 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, DPRI appears to have reasonable to strong controls in most areas. Three opportunities for improvement were noted.

**Information Security Systems - Automatic Computer Updates**
The three computers tested required administrator access to install automatic updates. One of the computers tested did not have current updates. There is an increased risk that computers will not be updated in a timely manner if the updates are not installed automatically and administrator access is required to install the updates.

Section 4.5.5.2 of UT Austin’s Minimum Security Standards for Systems states that “operating system and application services security patches should be installed expediently.”

| **Recommendation 1:** Management should configure all computers to automatically install updates when they become available. |
| **Management Response:** We agree with this recommendation and are implementing Absolute Manage, the recommended tool for managing desktop computers at UT Austin, on all desktop computers at DPRI. This will ensure that all updates are automatically installed as they become available. |
| Using Absolute Mange we will configure all computers so that updates are automatically installed as they become available. Upon completion of the configuration process we will run tests to ensure that the update function is in place and working on all computers. |
| **Implementation Date:** We will ensure that all computers are automatically updated by October 1, 2012. |

**Information Security Systems - Position of Special Trust Forms**
Positions with access to Category I data have not been designated as such in the Human Resource Management System (HRMS). As a result, employees in those positions have not have completed the Position of Special Trust form. If the form is not completed, employees may 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 2:** 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:** We agree with this recommendation and are currently ensuring that all positions with access to Category 1 data are so designated in the HRMS system.

DPRI is in the process of hiring an IT Manager and will ensure that this position is so designated as soon as the hiring process is complete and the new person is on staff.

**Implementation Date:** We will ensure that all positions with access to Category 1 data are so designated in the HRMS system by October 1, 2012.

**Information Systems Security - Securing Unattended Devices**

All three 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 3:** Management should ensure that all computers are configured with password protected screen savers that activate after 15 minutes of idle time.

**Management Response:** We agree with this recommendation and are implementing Absolute Manage, the recommended tool for managing desktop computers at UT Austin, on all computers at DPRI. This will ensure that all computers are configured with password protected screen savers that activate after 15 minutes of idle time.

Using Absolute Manage we will configure all computers with password protected screen savers that activate after 15 minutes of idle time. Upon completion of the configuration process we will run tests to ensure that password protected screen savers are functioning on all computers.

**Implementation Date:** We will ensure that all computers are configured with password protected screen savers that activate after 15 minutes by October 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 Andrew Keegan at 471-9836 or andrew.keegan@austin.utexas.edu.

MV: ak

Attachment

cc: Dr. Steven W. Leslie, Executive Vice President and Provost
    Dr. Charles A. Roeckle, 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 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>

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