Departmental Change in Management Audit
Fiscal Year 2013

March 2014

The University of Texas at Austin
Office of Internal Audits
UTA 2.302
(512) 471-7117
The University of Texas at Austin
Internal Audit Committee

Mr. William O’Hara, External Member, Chair
Mr. William C. Powers Jr., President
Dr. Gregory Fenves, 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
Ms. Mary E. Knight, CPA, Associate Vice President
Mr. Paul Liebman, Chief Compliance Officer, University Compliance Services
Mr. Cameron D. Beasley, University Information Security Officer
Mr. Tom Carter, External Member
Mr. Ben Mendez, External Member
Ms. Lynn Utter, External Member
Mr. Michael W. Vandervort, Director, Office of Internal Audits
Mr. J. Michael Peppers, Chief Audit Executive, University of Texas System

The University of Texas at Austin
Office of Internal Audits

Director: Michael Vandervort, CPA
Assistant Directors:
* Angela McCarter, CIA, CRMA
  Chris Taylor, CIA, CISA
Auditor III:
  Ashley Foster, CPA
  Brenda Guerrero
  Cameosha Jones
Auditor II:
  Miranda Pruett
  * Derek Stuart
Auditor I:
  Cameron Fletcher
  Stephanie Grayson
  Cynthia Martin-Hajmasy
Sr. IT Auditor:
  Tod Maxwell, CISA, CISSP
IT Auditor:
  Brandon Morales, CISA, CGAP
  Amber Whelpley, CIA, 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 Audit
Project Number: 805.13
March 28, 2014

President William C. Powers, Jr.
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 FY13 Change in Management Audit. Our scope included eight units selected based on a risk assessment and changes in departmental management as part of our Fiscal Year 2013 Audit Plan. Our audit process included surveying department heads by questionnaire, interviewing management and staff in each unit, reviewing electronic office structure, and transaction testing.

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

4000-000 Office of the Vice President for Student Affairs

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: Dr. Gage Paine
Vice President for Student Affairs

From: Mr. Michael Vandervort, CPA
Director

Subject: Final Report – Change in Management Audit, Fiscal Year 2013
Unit #4000-000: Office of the Vice President for Student Affairs (Project 
# 805.13)

Date: March 28, 2014

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

We reviewed internal controls in the following areas:

- Electronic Office Structure,
- General Departmental
  Information/Organization/Activities,
- Account Reconciliations,
- Outside Employment/Conflict of 
  Interest,
- Cash and Cash Equivalent Handling,
- Inventory,
- Purchasing Activities,
- Procurement Cards,
- Travel Expenditures,
- Entertainment and Official 
  Occasion Expenditures,
- Authorization for Individual 
  Services,
- Contracts,
- Time Reporting, and
- Information Systems Security.

We performed the following procedures to complete this audit:

- Surveyed via a questionnaire to ascertain your reported strength in internal 
  controls and compliance with UT Austin rules;
- Tested account certifications, entertainment and official occasion, travel and 
  procard transactions, annual physical inventory completion, and information 
  systems security;
- Reviewed your electronic office structure and employees’ appointment statuses; 
  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, the Office of the Vice President for Student Affairs (VPSA) appears to have reasonable to strong controls in most areas. Seven opportunities for improvement are noted.

**Information Systems Security – Administrative Access**

Department personnel stated in a meeting that faculty and staff have administrative access to their machines. When users operate with administrative rights at all times, it is difficult to protect against unauthorized access to data, software installations, and system configuration changes to workstations. This particular issue is preeminent among our opportunities for improvement because improperly granted administrative access cascades down to other issues which may not exist if administrative privileges were not accessible, namely: Position of Special Trust Form, Securing Category-I Digital Data, Securing Unattended Devices, and File Sharing. In other words, if administrative access was managed appropriately, four of the seven findings in this audit may not exist.

According to Section 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.”

<table>
<thead>
<tr>
<th>Recommendation 1:</th>
<th>Management should ensure that users operate workstations with the least privileges necessary to conduct business-related functions. Users with administrator privileges should use separate computer accounts only to perform administrative functions and not for day-to-day activities.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management Response:</strong></td>
<td>We are in the process of completing the addition of separate administrator accounts on all computers. All new computers are currently installed with separate administrator accounts and existing desktops will be converted by the end of January, 2014.</td>
</tr>
<tr>
<td><strong>Implementation Date:</strong></td>
<td>Implemented (Confirmed at follow-up testing on March 7, 2014)</td>
</tr>
</tbody>
</table>

**Information Systems Security – Position of Special Trust Form**

In addition to all staff having administrative access to their computers, departmental IT personnel indicated that all computers are configured as Category-I machines because data subject to the Family Educational Rights and Privacy Act (FERPA) is used in the department. However, only two individuals have been designated as having a Position of Special Trust (PoST) in the Human Resource Management System (HRMS).

---

If the PoST 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.

According to Section 5.4.4 of UT Austin’s *Information Resources Use and Security Policy*, “All individuals whose accounts have special privileges must complete a UT Austin Security Sensitive form. Additionally, all individuals assigned special privileges should acknowledge their responsibilities by signing a form such as a [PoST] form.”

**Recommendation 2:** Management should ensure that all individuals with access to Category I data are designated as such in HRMS and complete a PoST form annually.

**Management Response:** Effective immediately, all staff with access to Category I data will be designated as such in HRMS and will complete the PoST form annually.

**Implementation Date:** Implemented (January 31, 2014)

---

**Information Systems Security – Disaster Recovery Plan, Backup Recovery of Systems and Data**

The VPSA Disaster Recovery Plan (DRP) has not been updated since 2008 and is not being tested on an annual basis. Without an updated DRP, VPSA may not be able to adequately recover critical systems and data in the event of a disaster.

According to Section 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 [DRP]. The recovery plan includes the following:

- Procedures for recovering data and applications in case an unexpected event occurs such as natural disaster, power or system disk failure, espionage, data entry error, human error, or other systems operations 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;
- Processes to ensure backups are viable and can be recovered (for example, routine testing of backup and recovery procedures).”

**Recommendation 3:** Management should ensure that a comprehensive documented DRP exists within UT Austin’s Restarting Texas DRP application for all critical information resources and that it is tested at

---

2 Category-I Data is, “Data protected specifically by federal or state law or University of Texas rules and regulations...[and] data that are not otherwise protected by a known civil statute or regulation, but which must be protected due to contractual agreements requiring confidentiality, integrity, or availability considerations.” [http://security.utexas.edu/policies/data_classification.html](http://security.utexas.edu/policies/data_classification.html)

3 Restarting Texas is an application provided by the Information Security Office and is designed for departmental disaster recovery planning.
least annually. Additionally, the DRP should be kept up-to-date as staff and/or systems change.

**Management Response:** We completed our plan on October 31, 2013. Our plan will be kept up-to-date and will be tested annually.

**Implementation Date:** Implemented (October 31, 2013)

**Information Systems Security – Securing Category-I Digital Data**

Users can store and modify FERPA data on their own machines, which they have the ability to manage themselves. Consequently, the department may have Category-I data stored on unsecured machines. Without ensuring that Category-I data is secure at all times, there is an increased risk of data being compromised.

According to Section 5.11.3.3 of UT Austin’s *Information Resources Use and Security Policy*, “Unless otherwise required by federal or state law or regulation, Category-I Digital Data must not be stored, processed, or transmitted on university or non-university owned computers or other electronic devices (for example, laptop, hand-held device, Flash drive, or other portable computing devices) unless:

- It is secured against unauthorized access in accordance with this Policy;
- It will not compromise business or Research efforts or privacy interests if lost or destroyed; and
- The university has specific procedures in place that address this subsection.”

**Recommendation 4:** Management should create a more centrally managed computing environment that ensures all Category-I data is identified and secured on all devices.

**Management Response:** We will establish a more centrally managed computing environment by creating new VPSA policies which will require proof of a screen lock PIN, password or swipe pattern on smart phones on which UT Email is available. Also, we will not allow staff to use flash drives to store or share Category-I data; instead we will require staff to share data files via Austin Disk or UTBox. In addition, all laptops are encrypted according to policy, new or re-imaged desktops are encrypted, all other desktops will be encrypted according to policy, and iPads are password protected.

**Implementation Date:** Implemented (January 17, 2014)

**Information Systems Security – Securing Unattended Devices**

One of four computers tested did not have the password-protected screen saver settings enabled. 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.
Paine Memorandum
March 28, 2014
Page 5 of 7

According to Section 5.18.5 of UT Austin’s *Information Resources Use and Security Policy*, “Unattended computer devices must be secured from unauthorized access... Logical security options include screen saver passwords and automatic session time-outs.”

As a best practice, password-protected screen savers should activate after 15 minutes of idle time.

**Recommendation 5:** Management should ensure that the password-protected screen saver settings are enabled to activate after 15 minutes of idle time.

**Management Response:** The screen saver setting was not enabled on one of our Macs. That device has been updated on January 15, 2014 and we confirmed that all other Macs have enabled screen saver settings. The screen saver settings on Windows machines are controlled by ITSM group policy. It activates after 15 minutes of idle time and locks the computer, requiring password on wake.

**Implementation Date:** Implemented (Confirmed at follow-up testing on March 7, 2014)

**Information Systems Security – File-Sharing**

Two of four computers tested were configured to share files. Unauthorized access to data may result in harmful or fraudulent disclosure, modification, or deletion of confidential electronic data.

According to Section 5.3.5 of UT Austin’s *Minimum Security Standards for Data Stewardship*, “All university employees handling university data should avoid accessing, manipulating, or changing university data without the authorization of their supervisor or if is not required to fulfill assigned university duties. Such misuse includes... circumventing the assigned levels of data access given to other users by providing access or data sets that are broader than those available via normal approved levels of access.”

**Recommendation 6:** Management should ensure that users do not share files from their computers.

**Management Response:** We identified two Macs that were configured to share files; the setting has been disabled as of January 15, 2014. We will provide a new VPSA policy to staff that disallows file sharing from computers and requires files to be shared on Austin Disk or UT Box.

**Implementation Date:** Implemented (Confirmed at follow-up testing on March 28, 2014)

---

4 The UT Austin *Minimum Security Standards for Data Stewardship*: [http://security.utexas.edu/policies/standards_stewardship.html#section_5](http://security.utexas.edu/policies/standards_stewardship.html#section_5)
Information Systems Security – Firewalls
Testing indicated that one of the four computers had firewalls configured to allow all incoming connections and is also classified as a Category-I device within the Information Security Office Risk Assessment Report. Computers that do not limit connections are at a much higher risk of being compromised and may lead to the unauthorized access, modification, or disclosure of confidential data.

According to Section 4.5.5 of UT Austin’s Minimum Security Standards for Systems⁵, “Methods should be enabled to limit connections to services running on the host to only the authorized users of the service. Software firewalls, hardware firewalls, and service configuration are a few of the methods that may be employed.”

In addition, all Category-I designated computers are required to implement the rule.

<table>
<thead>
<tr>
<th>Recommendation 7: Management should ensure that all computers have firewalls configured to limit incoming connections.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Response: We identified one Mac that was not configured properly; it was updated on January 15, 2014. All Macs have the firewall enabled and the Windows firewall is enabled and configured by ITSM group policy.</td>
</tr>
<tr>
<td>Implementation Date: Implemented (Confirmed at follow-up testing on March 7, 2014)</td>
</tr>
</tbody>
</table>

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 Derek Stuart at 512-471-8896 or derek.stuart@austin.utexas.edu.

MV: ds

Attachment

⁵ The UT Austin Minimum Security Standards for Systems: http://security.utexas.edu/policies/standards_systems.html#section_4
Change in Management Report Card  
Office of the Vice President for Student Affairs, Unit #4000-000

<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;6&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 Systems Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<sup>6</sup> A weakness that significantly impacts UT Austin’s operations or finances