Department Change in Management Audits Fiscal Year 2012

February 2013

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. Clay R. Simmons, Interim 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: Angela McCarter, CIA, CRMA
*Chris Taylor, CIA, CISA
Auditor III: *Brenda Guerrero
Auditor II: Caroline Poquez
Auditor I: Ashley Foster
Cameosha Jones
Miranda Pruett
Derek Stuart
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
February 26, 2013

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 have completed two additional audits of departmental units at the University. 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.

Due to the individual nature of each review, we have attached the following reports for your information:

3590-000 Petroleum Extension Services
0680-000 Department of Sociology

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. Christine Williams, Department Chair  
Department of Sociology

From: Mr. Michael Vandervort, CPA  
Director

Subject: Final Report – Change in Management Audit, Fiscal Year 2012  
Unit #0680-000: Department of Sociology

Date: February 25, 2013

We have completed our audit of your compliance with and awareness of certain policies and procedures of The 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,
- Inventory,
- Purchasing Activities,
- Procurement Cards,
- Travel Expenditures,
- Entertainment and Official Occasion Expenditures,
- Time Reporting, and
- Information System 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 information system security, entertainment and official occasion transactions, endowment transactions, and annual physical inventory completion;
- 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 Department of Sociology appears to have reasonable to strong controls in most areas. Six opportunities for improvement are noted.

**Information System Security – Securing Unattended Devices**

Testing indicated that five of five computers did not have the password-protected screensaver setting 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.

According to Section 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 timeouts.”

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

**Recommendation 1:** Management should ensure that the password-protected screensaver settings are enabled and activate after 15 minutes of idle time.

**Management Response:** The Executive Assistant distributed an email to all staff to ask them to enable screensaver passwords. Sociology On-Site Computing Support will enable Active Directory user domain policy settings that will enforce password-protected screensaver activation after 15 minutes for all Windows systems. Users of Macintosh systems will be instructed on password-protected screensaver activation and university policy requirements.

**Implementation Date:** Implemented (1/02/13)

**Information System Security – Administrative Access**

The IT staff indicated that when users are given administrative rights to a machine, a separate account without administrative right is not created. 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.

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 2:** Management should ensure that users do not operate workstations with administrative rights unless required for a specific business function. If determined necessary, a new user account with administrative rights should be created and used to perform administrative functions apart from their day-to-day activities.
Management Response: Sociology On-Site Computing Support will change all staff accounts from administrative to standard users. Faculty admin accounts will be changed from Admin to standard user accounts where possible and exceptions will be documented. Sociology users who have admin level privileges will be identified and documented. Computing Services will create a log of users who have administrative access and will require Chair approval for this level of access in the future. Sociology Management will require and then verify that all users who have administrative access have completed the Position of Special Trust form.

Implementation Date: Implemented (1/2/13)

Information System Security – Firewalls
Testing indicated that three of the five computers had firewalls configured to allow all incoming connections. Of the three computers, two are classified as Category I devices 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 Systems, “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.

Recommendation 3: Management should ensure that all computers have firewalls configured to limit incoming connections.

Management Response: Sociology On-Site Computing Support currently enables Active Directory domain policy settings that require local firewalls on Windows Based Systems. For Macintosh based systems, Computing Support will ensure that the firewall is turned on at system setup and document that in System Setup Checklists that will be kept on file in the Computing Services office suite (CLA 2.602).

Implementation Date: Implemented (1/2/13)

Entertainment and Official Occasion Expenses – Itemized Receipts
Two of the five transactions tested were for catering, and an itemized receipt was not included in the supporting documentation.

According to Section 9.1.1.K.1.e of UT Austin’s Handbook of Business Procedures, for entertainment and official occasion expenses, “an itemized receipt or ticket is required for meals, or events with food, and the receipt or ticket must include the number of attendees. If an itemized receipt or ticket is not available, a statement declaring this must be included either on the OOE, the non-itemized receipt, or in the Notes section of the
electronic document, and the unit business officer, unit head, director, chair, or official delegate must approve the expense.”

**Recommendation 4:** Management should ensure that entertainment and official occasion expenses are supported with an itemized receipt for meals and events with food. If itemized receipts are not available, a statement declaring this must be included in the supporting documentation.

**Management Response:** The Executive Assistant reviewed the requirements with the Administrative Associate responsible for OOEF items.

**Implementation Date:** Implemented (12/10/12)

**Purchasing Activities**
The employee who purchases goods also receives the goods when they are delivered. Without proper separation of duties, there is an increased risk of theft or loss of items.

As a best practice, the purchase of goods and receipt of the goods should be delegated to two different employees.

**Recommendation 5:** Management should ensure that one employee other than the employee making the purchase confirms receipt of goods.

**Management Response:** The Executive Assistant alerted all staff regarding this requirement.

**Implementation Date:** Implemented (12/10/12)

**Cash and Cash Equivalent Handling – Locked Bag**
A locked bag is not used to transport funds to the Bursar’s Office for deposit. When a locked bag is not used, there is an increased risk of loss of funds.

According to the Cash Handling section of *The University of Texas System Policy 166*, “All cash, physical checks and receipts should be transported in tamper proof bags.”

**Recommendation 6:** Management should ensure that a locked bag is used when transporting funds.

**Management Response:** The department will purchase a locked bag.

**Implementation Date:** Implemented (1/2/13)
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 Brenda Guerrero at 471-9256 or brenda.guerrero@austin.utexas.edu.

MV: bg

Attachment

cc:       Dr. Randy Diehl, Dean, College of Liberal Arts
          Dr. Steven 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 Weaknesses(^1)</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/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