FY 2014 Departmental Change in Management Audit

Chemical Engineering

May 2015

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, Independent Member, Chair
Mr. William C. Powers Jr., President
Dr. Gregory Fenves, Executive Vice President and Provost
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 and Interim Chief Financial Officer
Mr. Paul Liebman, Chief Compliance Officer, University Compliance Services
Mr. Cameron D. Beasley, University Information Security Officer
Mr. Tom Carter, Independent Member
Ms. Lynn Utter, Independent 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
Associate Director Jeff Treichel, CPA
Assistant Directors: Angela McCarter, CIA, CRMA
Auditor III: *Chris Taylor, CIA, CISA
Auditor II: *Cameosha Jones
Cynthia Martin-Hajmasy, CPA
Ashley Oheim, CPA
Auditor I: Stephanie Grayson
Miranda Pruett, CFE
Sr. IT Auditor: Jason Boone
Bobby Castillo
Kerri Jordan
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.

FY 2014 Departmental Change in Management Audit: Chemical Engineering
Project Number: 14.103
May 28, 2015

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 our audit of Chemical Engineering (CHE). Our scope included controls and operations in place for fiscal year 2014.

Based on the audit procedures performed, we conclude that CHE has reasonable to strong controls in most of the areas reviewed. However, opportunities for improvement were noted in general departmental information/organization/activities, information systems security, cash and cash equivalent handling, and purchasing. Our audit report provides detailed observations for each area under review. Suggestions are offered throughout the report for improvement in the existing control structure.

We appreciated the cooperation and assistance of CHE throughout the audit and hope that the information presented herein is beneficial.

Sincerely,

Michael W. Vandervort, CPA
Director

cc: Internal Audit Committee Members
Ms. Nancy Brazzil, Deputy to the President and Chief of Staff
Dr. Sharon Wood, Dean, Cockrell School of Engineering
Dr. Thomas Truskett, Department Chair, Chemical Engineering
Mr. Jeff Treichel, Associate Director, Office of Internal Audits
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td>Background</td>
<td>2</td>
</tr>
<tr>
<td>Scope, Objectives, and Procedures</td>
<td>2</td>
</tr>
<tr>
<td>Audit Results</td>
<td>3</td>
</tr>
<tr>
<td>Conclusion</td>
<td>8</td>
</tr>
<tr>
<td>Appendix</td>
<td>9</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Conclusion
Based on the audit procedures performed, we conclude that Chemical Engineering (CHE) has reasonable to strong controls in most of the areas reviewed. However, opportunities for improvement were noted in general departmental information/organization/activities, information systems security, cash and cash equivalent handling, and purchasing.

Summary of Recommendations
Internal Audits identified two notable issues which led to the following recommendations:

- Ensure that a records management plan is developed and maintained; and
- Ensure that a comprehensive disaster recovery plan exists.

Five additional recommendations are provided, but are considered minor in significance.

Management agrees with our observations and has provided corrective action plans which are expected to be implemented on or before September 30, 2015.

Audit Scope and Objective
Departmental Change in Management audits are conducted annually and units are chosen based on a risk assessment. The objective is to evaluate the adequacy and effectiveness of the unit’s structure, processes, and internal controls and to determine compliance with relevant policies and procedures for fiscal year 2014.

Background Summary
CHE was established at The University of Texas at Austin in 1915. CHE currently has four department administrators, 21 staff members, and 39 faculty members. CHE has a budget of approximately $6.3 million and is a part of the Cockrell School of Engineering.
BACKGROUND

Chemical Engineering (CHE) was established at The University of Texas at Austin (UT Austin) in 1915. CHE generates $20 million in annual research funding and manages strong programs in several areas. Faculty research programs have generated six successful start-up companies to commercialize findings.

The unit hosts 53 research labs, two undergraduate labs, three computer labs, a polymers lab, and a scanning electron microscope on UT Austin’s main campus. CHE currently has four department administrators, 21 staff members, and 39 faculty members. CHE has a budget of approximately $6.3 million and is a part of the Cockrell School of Engineering.

For management of IT resources, CHE uses internal IT staff. The department has approximately 736 computers and uses Microsoft and Apple operating systems. Thirty of the systems were reported to contain Category I data. In 2013, CHE had 10 breaches (i.e. remote attacker obtains unauthorized control of a system), constituting approximately one breach per 74 computers, which is consistent with the campus-wide average of one breach per 77 computers.

SCOPE, OBJECTIVES, AND PROCEDURES

The scope of this review includes controls and operations of the department currently in place for fiscal year 2014. Our objectives were to evaluate the adequacy and effectiveness of the unit’s structure, processes, and internal controls and to determine compliance with relevant policies and procedures.

To achieve these objectives, Internal Audits:

- Surveyed the unit via a questionnaire to ascertain reported strength in internal controls and compliance with UT Austin rules;
- Reviewed the department’s electronic office structure and employees’ appointment statuses;
- Conducted limited testing on account certifications, account reconciliations, cash and cash equivalent handling, payroll/HR, petty cash, inventory, purchasing, procurement card expenditures, travel expenditures, entertainment and official occasion expenditures, and information systems security; and
- Clarified follow-up issues through e-mails, meetings, and other correspondence.

This audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing and with Government Auditing Standards.
AUDIT RESULTS

We reviewed internal controls in 20 areas regarding departmental operations, financial processes, and information technology, of which five areas were not applicable to CHE. The appendix provides information on the specific areas reviewed. The following were the results:

- 11 (73\%) areas had reasonable to strong controls in place,
- 2 (13\%) areas had opportunities for minor improvements,
- 2 (13\%) areas had opportunities for significant improvements, and
- 0 (0 \%) areas had priority weaknesses.

Recommendations were made in areas where opportunities for improvements were noted and these are detailed in the remainder of this report.

General Departmental Information/Organization/Activities – Records Management Plan

The unit currently does not have a records management plan. The unit understood following the records management plan in the Handbook of Business Procedures was sufficient. Without having a records management plan in place, there is an increased risk that the department is not following UT Austin’s records management policy.

According to Section 20.4.2 of UT Austin’s Handbook of Business Procedures, “Each departmental records management contact (DRMC) at The University of Texas at Austin is responsible for creating a records management plan to provide information about how the department will enact university records management policy.”

**Recommendation 1:** Management should ensure that a records management plan is developed and maintained on file.

**Management’s Corrective Action Plan:**

1. Area staff leaders will meet with Mary Rose Hightower-Coyle, Office of Accounting Records Management Officer, May 20 at CPE to go over the plan development and inventory process, providing templates and examples.
2. Smaller work groups will be divided into inventory and plan development, as the plan will very much depend on the types and scope of records the department maintains, such as Financial, Human Resources, Academic, and Research.
3. Ms. Hightower-Coyle assures us we can have a plan in place within a month and our goal for both the plan and inventory to with it is 31 August 2015. She feels these are reasonable goals.

**Responsible Person:** Executive Assistant  
**Planned Implementation Date:** August 31, 2015
Information Systems Security – Disaster Recovery Plan (DRP) Backup Recovery of Systems and Data

The unit’s DRP is incomplete and is not being tested on an annual basis. Resources had not been devoted to completing a plan. Without an updated DRP, the unit 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 2: Management should ensure that a comprehensive documented DRP exists within UT Austin’s Kuali Ready DRP application\(^1\) for all critical information resources and that it is tested at least annually. Additionally, the DRP should be kept up-to-date as staff and/or systems change.

Management’s Corrective Action Plan: We will develop a comprehensive DRP within UT Austin’s Kuali Ready DRP Application. This application will be kept up-to-date with any personnel changes and any systems changes. Once developed, we will test annually as per recommendation. This testing will be performed during the annual ISORA timeframe.

Responsible Person: Senior Information Technology Manager
Planned Implementation Date: September 30, 2015

Post Audit Review: Internal Audits will perform follow-up work once the implementation date has passed.

---

\(^1\) Kuali Ready is an application provided by the Information Security Office and is designed for departmental disaster recovery planning.
Information Systems Security – Securing Unattended Devices
Password-protected screensavers are not currently set to activate after 15 minutes of inactivity. The unit stated that password-protected screensavers were set to activate after 30 minutes of idle time; this was confirmed during testing. Unauthorized access to unattended devices may result in harmful or fraudulent disclosure, modification, or deletion of sensitive electronic data. In addition, this 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 controls include screen saver passwords and automatic session time-outs that are set to activate after 15-minutes of inactivity.”

Recommendation 3: Management should ensure that the password-protected screensaver settings are enabled to activate after 15 minutes of inactivity.

Management’s Corrective Action Plan: The department will be given advanced notice of the changes a few days ahead of time. We will modify the Active Directory Group Policy password-protected screensaver activation from 30 minutes to 15 minutes. We will randomly check a few PCs to verify the password-protected times have changed to 15 minutes.

Responsible Person: Senior Information Technology Manager and Systems Administrator I
Planned Implementation Date: May 22, 2015

Post Audit Review: Internal Audits will perform follow-up work once the implementation date has passed.

Information Systems Security – Compliance Training
At the time of testing, 18 (6%) of 308 departmental employees tested had not completed TX Class CW 170 – IT Security Awareness training. The unit does not currently have practices in place to ensure that all employees complete required training. There is an increased risk of security incidents if employees are not properly trained regarding the use of departmental information technology resources.

According to Section 5.22 of UT Austin’s Information Resources Use and Security Policy, all employees are required to take security awareness General Compliance training within the first 30 days of employment and every two years thereafter.

Recommendation 4: 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’s Corrective Action Plan:** During the onboarding process, all new employees will be directed to the New Employee Checklist or New Student Employee Checklist as appropriate to inform them of the required actions. Onboarding staff will follow-up with reminders, cc’ing supervisors, until all have completed this course.

**Responsible Person:** Executive Assistant  
**Planned Implementation Date:** Immediately (May 15, 2015)

**Post Audit Review:** Internal Audits is in the process of performing follow-up work.

---

**Information Systems Security – Position of Special Trust (PoST)**

At the time of testing, 5 (15%) of the 33 employees whose position is designated as having access to Category I data have not completed PoST forms. The unit does not have a procedure in place to ensure that all employees whose positions are flagged as requiring a PoST on file complete the required 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.

According to the Information Security Office website, “in accordance with The University of Texas at Austin Information Resources and Security Policy (section V, item 4), 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.”

**Recommendation 5:** Management should ensure that all individuals with access to Category I data complete a PoST form annually.

**Management’s Corrective Action Plan:** During the onboarding process, all new employees will be directed to the New Employee Checklist or New Student Employee Checklist as appropriate to inform them of the required actions. Onboarding staff will follow-up with reminders, cc’ing supervisors, until all have completed this requirement. Once an employee has reached the 30 day deadline and is out of compliance, all follow-up will be conducted by the Department Executive Assistant and main HR contact, Karen Eikner.

**Responsible Person:** Executive Assistant  
**Planned Implementation Date:** Immediately (May 15, 2015)

**Post Audit Review:** Internal Audits is in the process of performing follow-up work.

---

2 Information Security Office website - [https://security.utexas.edu/specialtrust/about/](https://security.utexas.edu/specialtrust/about/)
Cash and Cash Equivalent Handling – Timely Deposits
One (33%) out of the three deposit transactions tested was not deposited within the required timeframe. The unit stated that checks are sometimes held in the safe for a long period of time because it is not clear which account the checks should be deposited into. If deposits are not made in a timely manner, there is an increased risk of lost funds.

According to Section 6.5.B of UT Austin’s *Handbook of Business Procedures*, “Deposits should be made daily if they are equal to or greater than $500. Deposits should be made at least weekly even if the accumulated total is less than $500.”

**Recommendation 6:** Management should ensure that cash and cash equivalents of $500 or more are deposited daily at the Bursar’s Office and that all cash and cash equivalents are deposited at least weekly even if the accumulated total is less than $500.

**Management’s Corrective Action Plan:** The Cash and Cash Equivalent Handling Process involves the efforts of Procurement, Accounts Payable, and the Financial Analyst. All involved have been made aware of the requirement to deposit cash and cash equivalents valued $500 or more within 24 hours, and at least weekly if the accumulated total is less than $500.

Upon receipt of a cash instrument, Accounts Payable will log the check in the CHE Deposit Database, and notify Procurement and the Financial Analyst of the required processing timeline (based upon accumulated value of pending deposits.) Procurement will create the required transaction in DEFINE, and route the document to the Financial Analyst for approval. Procurement is responsible for ensuring the check is then deposited at the Cashier’s Office or the Development Office as appropriate.

**Responsible Person:** Financial Analyst, Administrative Associate (Accounts Payable), Senior Administrative Associate (Procurement)

**Planned Implementation Date:** Immediately (May 15, 2015)

**Post Audit Review:** Internal Audits is in the process of performing follow-up work.

Purchasing – Receiving Goods/Services
The unit currently uses a stamp without a signature to mark goods and services as received. The unit believed the stamp without a signature was sufficient to document the goods and services received. Without a signature of the individual verifying the receipt of goods/services, accountability and separation of duties cannot be assured.
According to UT Austin’s Purchasing Office website, “For shipments received in the department, receipt must be evidenced by notation on the original itemized invoice of the date of receipt and the signature of the individual that received the shipment.”

**Recommendation 7:** Management should ensure that evidence of goods/services received is documented with a signature and date of the responsible individual.

**Management’s Corrective Action Plan:** The original itemized invoices of all good/services received will be signed and dated by the responsible individual upon receipt.

**Responsible Person:** Laboratory/Technical Services Supervisor I  
**Planned Implementation Date:** Immediately (May 15, 2015)

**Post Audit Review:** Internal Audits is in the process of performing follow-up work.

**CONCLUSION**

Based on the audit procedures performed, we conclude that Chemical Engineering (CHE) has reasonable to strong controls in most of the areas reviewed. However, opportunities for improvement were noted in general departmental information/organization/activities, information systems security, cash and cash equivalent handling, and purchasing.

In accordance with directives from The University of Texas System Board of Regents, the Office of Internal Audits will perform follow-up procedures to confirm that audit recommendations have been implemented.

---

1 Purchasing Website: [http://www.utexas.edu/admin/purchasing/receiving.html](http://www.utexas.edu/admin/purchasing/receiving.html)
## APPENDIX

<table>
<thead>
<tr>
<th>Area</th>
<th>Reasonable Controls in Place</th>
<th>Opportunity for Minor Improvements</th>
<th>Opportunity for Significant Improvements</th>
<th>Priority Weakness [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>Payroll/HR</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 and Cash Equivalent Handling</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>Petty Cash</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>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>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>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>Information Systems Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[1] A priority weakness, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole. These findings will be reported to UT System Administration.