The University of Texas at Austin
Internal Audit Committee

Mr. William O’Hara, Independent Member, Chair
Dr. Gregory L. Fenves, President
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
*Chris Taylor, CIA, CISA
Audit Manager: Brandon Morales, CISA, CGAP
Auditor III: Michael Hammond, CIA, CISA, CFE
Cynthia Martin-Hajmasy, CPA
Ashley Oheim, CPA
Auditor II: Stephanie Grayson
Miranda Pruett, CFE
Auditor I: Jason Boone
Bobby Castillo
Kerri Jordan
Sr. IT Auditor: *Tod Maxwell, CISA, CISSP
IT Auditor: Tiffany Yanagawa
* 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.

Information Technology General Controls: College of Natural Sciences
Project Number: 14.301
August 31, 2015

President Gregory L. Fenves
The University of Texas at Austin
Office of the President
P.O. Box T
Austin, Texas 78713

Dear President Fenves,

We have completed our audit of the College of Natural Sciences (CNS). Our scope included current IT controls within CNS.

Based on the audit procedures performed, we conclude that CNS’s IT management practices minimize risk and are in compliance with most applicable policies and standards. 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 appreciate the cooperation and assistance of CNS throughout the audit and hope that the information presented herein is beneficial.

Sincerely,

Michael W. Vandervort, CPA
Director

cc: Internal Audit Committee Members
    Dr. Linda Hicke, Dean, College of Natural Sciences
    Ms. Patricia Ohlendorf, Vice President for Legal Affairs
    Mr. Jeff Treichel, Associate Director, Office of Internal Audits
# TABLE OF CONTENTS

Executive Summary ........................................................................................................... 1

Background ......................................................................................................................... 2

Scope, Objectives, and Procedures ..................................................................................... 3

Audit Results ....................................................................................................................... 4

Conclusion .......................................................................................................................... 8

Appendix ............................................................................................................................. 9
EXECUTIVE SUMMARY

Conclusion
Based on the audit procedures performed, the Office of Internal Audits (Internal Audits) concludes that the College of Natural Sciences (CNS) information technology management practices minimize risk and are in compliance with most applicable policies and standards. We made five recommendations related to Backup and Disaster Recovery Plan, Management of Category I Data, Administrative/Special Access, Unattended Devices, and Awareness and Training.

Summary of Recommendations
Each issue has been ranked according to the University of Texas System Administration (UT System) Audit Issue Ranking guidelines. Please see the Appendix on the last page for ranking definitions. Internal Audits identified four notable issues which led to the following recommendations.

- Create a comprehensive disaster recovery plan (Audit Issue Ranking: High)
- Document critical IT processes and procedures (Audit Issue Ranking: High)
- Operate computers with the least privileges (Audit Issue Ranking: High)
- Enable automated password protected screensavers (Audit Issue Ranking: High)

One additional recommendation is provided, but is considered minor in significance.

Management agreed with our observations and has provided corrective action plans which are expected to be implemented on or before 6/1/2016.

Audit Scope and Objective
This audit was conducted as part of the Fiscal Year 2014 Audit Plan. The scope of the audit included current IT controls within CNS. The audit objective is to determine if CNS IT management practices minimize risk and are in compliance with applicable policies and standards.

Background Summary
CNS’ Office of Information Technology (CNS-OIT) provides computing services and support for ten of the college’s 11 departments. The ten departments comprise approximately 650 faculty, 1,100 administrative staff, and 11,500 students. At the time of our audit, CNS-OIT consisted of 37 full-time employees, including the Executive Director who reports to the Dean of CNS. CNS-OIT’s budget for FY14 totaled $3.4 million.
BACKGROUND

Information and related technology are critical assets enabling The University of Texas at Austin (UT Austin) to process, maintain, and report on vital operations. However, without appropriate controls, IT systems are at risk to unauthorized access, disclosure, or destruction of financial, academic, or research information.

Recognizing the importance of IT security, UT Austin created the Information Resources Use and Security Policy (IRUSP)\(^1\) in accordance with Federal and State law and Regents’ Rules and Regulations.

Technical Overview

In March 2013, the College of Natural Sciences (CNS) started an initiative to combine all of its unit-level IT support activities. By September 2014, ten of the college’s 11 IT units had joined to become the College of Natural Sciences’ Office of Information Technology (CNS-OIT). The Department of Computer Science is the only remaining department in CNS that manages its own IT resources.

CNS-OIT provides computing services and support for approximately 650 faculty, 1,100 staff, and 11,500 students located across 38 buildings. CNS-OIT is responsible for roughly 7,500 computing devices including 270 Category I systems. At the time of our audit, CNS-OIT consisted of an Executive Director overseeing 37 full-time employees and a $3.4 million budget.

Building Network Report Card\(^2\)

The ITS Networking Building Network Report Card provides an overview of each building’s compliance with minimum UT Austin network standards. Grades in the report relate to each network’s compliance, performance, and life cycle state. Networks tend to begin as an “A” and decay over time until grades approach a “D”, which illustrates the need for a systematic approach to managing network infrastructure. Buildings with more demanding users require an accelerated life cycle to keep networks at an “A” or “B” grade.

CNS Building Network Report Card as of 7/2015\(^3\)

\(^1\) [http://security.utexas.edu/policies/irusp.html](http://security.utexas.edu/policies/irusp.html) - UT Austin Information Resources Use and Security Policy

\(^2\) The ITS building network report card does not include CNS-OIT shared buildings.

\(^3\) A recommendation relating to MSI’s network score was covered in audit #817.13.
Security Incidents
An IT security incident as defined in the Information Security Office Risk Assessment (ISORA) can include items such as system compromises, high risk vulnerabilities, and policy violations. The following table provides a breakdown of business system compromises in each of CNS-OIT’s ISORA reporting departments as of August 2015. For comparison purposes, totals for CNS and all of UT Austin are provided for the current and last two years. Please note that system compromise information is based on calendar and not fiscal year.

CNS IT System Compromises Compared to All of Campus

<table>
<thead>
<tr>
<th>ISORA Reporting Departments</th>
<th>Compromises</th>
<th>Systems as of 12/2014</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>YTD as of 08/2015</td>
<td>2014</td>
</tr>
<tr>
<td>UT Austin Campus</td>
<td>583</td>
<td>1,329</td>
</tr>
<tr>
<td>CNS Dean’s Office</td>
<td>21</td>
<td>7</td>
</tr>
<tr>
<td>Astronomy</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>Biology Instructional</td>
<td>22</td>
<td>64</td>
</tr>
<tr>
<td>Chemistry</td>
<td>3</td>
<td>34</td>
</tr>
<tr>
<td>Computer Science</td>
<td>6</td>
<td>15</td>
</tr>
<tr>
<td>Human Ecology</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Nano/Molecular Science</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Marine Science</td>
<td>4</td>
<td>11</td>
</tr>
<tr>
<td>Mathematics</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Physics</td>
<td>18</td>
<td>26</td>
</tr>
<tr>
<td>CNS Totals</td>
<td>83</td>
<td>173</td>
</tr>
</tbody>
</table>

SCOPE, OBJECTIVES, AND PROCEDURES

The audit objective is to determine if CNS information technology management practices minimize risk and are in compliance with applicable policies and standards. The scope of the audit included current IT controls within CNS.

To achieve this objective, the Office of Internal Audits:
- Interviewed IT staff from CNS-OIT;
- Reviewed data from the Information Security Office Risk Assessment;
- Reviewed data from ITS-Networking;
- Reviewed CNS-OIT policies and procedures; and
- Conducted limited testing.

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

---

5 https://isora.security.utexas.edu – Information Security Office Risk Assessment
5 The Department of Computer Science statistics are included only for reference purposes and is not managed by CNS-OIT.
AUDIT RESULTS

We reviewed internal controls in 15 areas relating to CNS's information technology operations and processes. Ten of 15 areas had reasonable to strong controls in place in the following:

- Account Management
- Audit and Accountability
- Configuration Management
- Encryption
- Incident Response
- In-House Programming
- Inventory
- Passwords
- Risk Assessment
- Third-Party Access
- Inventory
- In-House Programming
- Inventory
- Passwords
- Risk Assessment

As part of CNS' initiative to combine IT operations, during the last 12 months, CNS-OIT management has worked to align each unit with UT Austin policies and procedures while improving upon their existing processes. For example, CNS-OIT has moved nearly all commodity and Category I servers physically located at units to the UT Austin University Data Center (UDC). In addition, CNS-OIT has coordinated with faculty to assume management of research related IT resources; re-engineered desktop, server, and application support activities; and strengthened IT risk assessment processes.

To further build on CNS's recent progress, Internal Audits made five recommendations in the following areas:

- Backup and Disaster Recovery Plan
- Unattended Devices
- Management of Category I Data
- Awareness and Training
- Administrative and Special Access

Each issue has been ranked according to the University of Texas System Administration (UT System) Audit Issue Ranking guidelines. Please see the Appendix on the last page for ranking definitions.

Backup and Disaster Recovery Plan
Audit Issue Ranking: High

CNS did not have a college-wide documented Disaster Recovery Plan (DRP). It appears recent organizational and process changes within CNS prevented the documentation of a college-wide DRP. Without a documented DRP in place, system administrators may not be able to adequately recover critical systems and data in the event of a disaster.

Rule 5.5.2 of UT Austin’s IRUSP states, “Each college, school, or unit responsible for a system(s) maintains 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 1:** CNS management should ensure that a comprehensive documented DRP exists within UT Austin’s Kuali Ready⁶ DRP application for all critical information resources and that it is updated and tested at least annually. Additionally, the DRP should be kept up-to-date as staff or systems change.

**Management’s Response and Corrective Action Plan:** We have already set up a project charter to complete the DRP and have identified a project lead and have established a project team. We prepared to do this project during the 2014-2015 and are ready to execute this year. We have moved most College servers to the UDC, with respect to CAT 1 data, have made it our practice not to operate servers that store or supply CAT 1 data.

**Responsible Person:** Executive Director of CNS-OIT

**Planned Implementation Date:** 6/1/2016

**Post Audit Review:** Internal Audits will follow-up in the fourth quarter of FY16.

---

**Management of Category I Data**

**Audit Issue Ranking:** High

A large portion of IT operations were not documented in CNS-OIT’s content management system including those associated with change management, user account creation, administrative account management, system configuration processes, and electronic data record retention. It appears recent organizational and process changes within CNS prevented the complete documentation of IT operations. Without documented procedures, organizations may find it difficult to manage, access, and utilize UT Austin data in a manner consistent with the need for confidentiality, integrity, and availability.

Rule 4 of UT Austin’s *Minimum Security Standards for Data Stewardship*⁷ states, “Each College, School, or Unit handling university data shall develop, maintain, and execute a data stewardship plan comprised of clear and consistent procedures describing how the respective area manages the handling, access, and protection of university data.”

**Recommendation 2:** CNS management should ensure that processes and procedures for critical IT activities are documented including but not limited to change management, user account creation, administrative account management, system configuration processes, and electronic data record retention. Written procedures should include sufficient information to permit an individual who is unfamiliar with the information technology operations to perform basic activities.

---

⁶ Kuali Ready - [https://us.ready.kuali.org/utexas](https://us.ready.kuali.org/utexas)
⁷ [http://security.utexas.edu/policies/standards_stewardship.html](http://security.utexas.edu/policies/standards_stewardship.html) - Minimum Security Standards for Data Stewardship
**Administrative and Special Access**

**Audit Issue Ranking: High**

Seven (41%) of the 17 CNS computers tested were configured allowing users to operate with administrator privileges. CNS computers may have been initially configured to allow users to operate with administrator privileges at all times. 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.

Rule 5.4.7 of UT Austin’s IRUSP states, “When access to a university-owned IT device’s administrative account is required by someone other than an IT Support Staff member, the following exception criteria must apply:

5.4.7.1. Individuals must annually complete the Position of Special Trust form;
5.4.7.2. Individuals must only use the administrative account for special administrative functions and default to a lower privileged user account for other day-to-day use;
5.4.7.3. Individuals must review the following training materials, How not to Login as Administrator (and still get your job done);
5.4.7.4. IT System Custodians are required to periodically review the use of administrative account exceptions.
   - 5.4.7.4.1. IT System Custodians will remove any administrative accounts that go unused or are no longer required; and
   - 5.4.7.4.2. IT System Custodians are required to raise inappropriate use to management (e.g., staying logged in with the administrative account longer than needed).”

**Recommendation 3:** CNS management should ensure users operate workstations with the least privileges necessary to conduct business related functions. If determined necessary, then a new user account with administrative rights should be created and used to perform administrative functions apart from day-to-day activities.

**Management’s Response and Corrective Action Plan:** We have begun the process of communicating with our users about this issue and have identified this issue as a top priority for the coming year. We will charter this project and execute it this year. We have already begun implementing a process of establishing new, throttled user accounts as we replace hardware. Administrative accounts must be requested.

**Responsible Person:** Executive Director of CNS-OIT

**Planned Implementation Date:** 6/1/2016
Post Audit Review: Internal Audits will follow-up in the fourth quarter of FY16.

Unattended Devices
Audit Issue Ranking: High
Nine (38%) of 17 CNS computers tested were configured without password-protected screensavers. CNS computers may have been deployed without 15 minute password protected screensaver enabled. Without password-protected screensavers that automatically time out, it is difficult to secure unattended devices. Unauthorized access to unattended devices can result in harmful or fraudulent disclosure, modification, or deletion of electronic data. In addition, this practice may lead to the misuse of critical applications or email accounts.

Rule 5.18.5 of The University of Texas at Austin’s IRUSP states, “Unattended computing devices must be secured from unauthorized access using a combination of physical and logical security controls commensurate with associated risks. Physical security controls include barriers such as locked doors or security cables. Logical security controls include screen saver passwords and automatic session time-outs that are set to activate after 15-minutes of inactivity.”

Recommendation 4: CNS management should enable the “require a password” on screensaver settings for all computers that activates after 15 minutes of idle time. Where applicable, CNS should use a centrally managed service such as Group Policy or Absolute Manage to enforce screensaver time-outs.

Management’s Response and Corrective Action Plan: We will establish a charter for this project and implement it during the coming year.
Responsible Person: Executive Director of CNS-OIT
Planned Implementation Date: 6/1/2016

Post Audit Review: Internal Audits will follow-up in the fourth quarter of FY16.

Awareness and Training
Audit Issue Ranking: Medium
Twenty-seven (4%) out of 648 faculty, staff, and student employees were past due with UT Austin’s CW170 - IT Security Awareness training when tested in February 2015. Faculty, staff, and student employees may not be overseen with regard to the completion of the CW170 module. There is an increased risk of security incidents when employees are not properly trained regarding the use of department information resources.

Section 5.22 of UT Austin’s IRUSP states, “The Information Security Office shall deliver security awareness General Compliance training in accordance with the following schedule:

5.22.1.1. Training of all Users, including students, with access to the university’s Information Resources shall take place biennially;
5.22.1.2. To each new, temporary, contract, assigned, or engaged employee or worker within 30 days after the date that such a person is (a) hired by university or (b) otherwise engaged or assigned to perform such work.”

**Recommendation 5:** CNS management should ensure that all employees complete TX Class CW170 – IT Security Awareness within 30 days of employment and every two years thereafter.

**Management’s Response and Corrective Action Plan:** We will establish a project charter for this finding and remediate this during the upcoming Fall semester. This plan will include communication from Dean Hicke to the College. We will then assist by answering questions and providing clarification.

**Responsible Person:** Executive Director of CNS-OIT

**Planned Implementation Date:** 12/1/2015

**Post Audit Review:** Internal Audits will follow-up in the second quarter of FY16.

**CONCLUSION**

Based on audit procedures performed, Internal Audits concludes that CNS information technology management practices minimize risk and are in compliance with most applicable policies and standards. We made five recommendations related to Backup and Disaster Recovery Plan, Management of Category I Data, Administrative/Special Access, Unattended Devices, and Awareness and Training.

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 agreed-upon audit recommendations have been implemented.
APPENDIX

Audit Issue Ranking

Audit issues are ranked according to the following definitions, consistent with UT System Audit Office guidance. These determinations are based on overall risk to UT System, UT Austin, and/or the individual college/school/unit if the issues are left uncorrected. These audit issues and rankings are directly reported to UT System.

- **Priority** – A Priority Issue is an issue that, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of UT Austin or the UT System as a whole.

- **High** – An issue that is considered to have a medium to high probability of adverse effects to UT Austin either as a whole or to a significant college/school/unit level.

- **Medium** – An issue that is considered to have a low to medium probability of adverse effects to UT Austin either as a whole or to a college/school/unit level.

- **Low** – An issue that is considered to have minimal probability of adverse effects to UT Austin either as a whole or to a college/school/unit level. Issues with a ranking of “Low” are reported verbally to the unit and are not included in the final report.